Request for Proposals

for

Security Operations Centre ("SOC") and Managed Detection and Response ("MDR") Provider

Request for Proposals No.: **21-735**

Issued: **August 30, 2021**

Submission Deadline**: October 13, 2021 at 12:00:00 PM local time**

TABLE OF CONTENTS

PART 1 – INVITATION AND SUBMISSION INSTRUCTIONS 3
1.1 Invitation to Proponents 3
1.2 RFP Contact 3
1.3 Contract for Deliverables 4
1.4 RFP Timetable 4
1.5 Submission Instructions 4
PART 2 – EVALUATION, NEGOTIATION, AND AWARD 6
2.1 Stages of Evaluation and Negotiation 6
2.2 Stage I – Mandatory Submission Requirements 6
2.3 Stage II – Evaluation 6
2.4 Stage III – Pricing 6
2.5 Stage IV – Initial Ranking, Short-Listing, and Interview Stage 7
2.6 Stage V – Contract Negotiations 7
PART 3 – TERMS AND CONDITIONS OF THE RFP PROCESS 9
3.1 General Information and Instructions 9
3.2 Communication after Issuance of RFP 10
3.3 Notification and Debriefing 10
3.4 Conflict of Interest and Prohibited Conduct 11
3.5 Confidential Information 13
3.6 Procurement Process Non-Binding 13
3.7 Governing Law and Interpretation 14
APPENDIX A – FORM OF AGREEMENT 15
APPENDIX B – RFP PARTICULARS 16
A. THE DELIVERABLES 16
B. MATERIAL DISCLOSURES 31
C. MANDATORY SUBMISSION REQUIREMENTS 33
D. MANDATORY TECHNICAL REQUIREMENTS 33
E. PRE-CONDITIONS OF AWARD 33
F. EVALUATION CRITERIA 33
G. PRICE EVALUATION METHOD 41
APPENDIX C – SUBMISSION FORM 45

FORM 1 – REFERENCE VALIDATION FORM

FORM 2 – DUE DILIGENCE QUESTIONNAIRE

PART 1 – INVITATION AND SUBMISSION INSTRUCTIONS

1.1 Invitation to Proponents

1.1.1 Invitation

This Request for Proposals (the "RFP") is an invitation by Export Development Canada ("EDC") to prospective proponents to submit proposals for a **Security Operations Center ("SOC") and Managed Detection and Response ("MDR") Provider** as further described in Section A of the RFP Particulars (Appendix B) (the "Deliverables").

EDC is seeking to contract with a SOC and MDR provider who will monitor the security of EDC's hybrid information technology ("IT") environment.

The provider will be required to:

- utilize Microsoft Azure Sentinel security information and event management ("SIEM") and security orchestration, automation, and response ("SOAR") platform, taking advantage of its full range of capabilities and integrations, while utilizing Azure Lighthouse to connect with EDC's Sentinel instance;
- configure Sentinel and guide EDC to configure existing and future IT assets in the public cloud, on-premises, or software as a service ("SaaS"), to ingest events and provide alert triage and incident escalation services correlated against an extensive range of threat intelligence and supported with extensive level of detail and guidance to EDC's computer security incident response ("CSIRT") and network operations centre ("NOC") teams;
- configure Sentinel SOAR to perform a range of low-risk, high-frequency, automated mitigations across the various EDC technology platforms listed in Appendix B.
- provide enhanced client dashboard and extensive regular reporting on the performance of its service and cybersecurity activities;
- lead with exceptional account and service management, complemented with industry vision and expertise, to drive continuous service improvements; and
- provide temporary monitoring of EDC's IBM QRadar platform until the bidder has fully onboarded all existing EDC assets into Sentinel.

1.1.2 Proponent Must Be Single Entity

The proponent must be a single legal entity that, if selected, intends to negotiate and enter into a contract with EDC. If the proposal is being submitted jointly by two (2) or more separate entities, the proposal must identify only one (1) of those entities as the "proponent". The proponent will be responsible for the performance of the Deliverables and will be subject to any associated liquidated damages in the event of non-compliance or non-delivery (Deliverable Liquidated Damages Tables (Section A. Deliverables of Appendix B – RFP Particulars)).

1.2 RFP Contact

For the purposes of this procurement process, the "RFP Contact" will be:

EDC_SOC-MDRRFP@procurementadvisor.ca

Proponents and their representatives are not permitted to contact any employees, officers, agents, elected or appointed officials, or other representatives of EDC, other than the RFP

Contact, concerning matters regarding this RFP. Failure to adhere to this rule may result in the disqualification of the proponent and the rejection of the proponent's proposal.

1.3 Contract for Deliverables

1.3.1 Type of Contract

The selected proponent will be requested to enter into direct contract negotiations to finalize an agreement with EDC for the provision of the Deliverables. The terms and conditions found in the Form of Agreement (Appendix A) are to form the basis for commencing negotiations between EDC and the selected proponent.

1.3.2 Term of Contract

The term of the agreement is to be for a period of three (3) years, with an option in favour of EDC to extend the agreement on the same terms and conditions for two (2) additional terms of up to one (1) year each.

1.4 RFP Timetable

1.4.1 Key Dates

Issue Date of RFP	August 30, 2021
Deadline for Questions	September 15, 2021 at 11:59:59 PM local time
Deadline for Issuing Addenda	September 29, 2021 at 11:59:59 PM local time
Submission Deadline	October 13, 2021 at 12:00:00 PM local time
Rectification Period	Three (3) business days
Anticipated Initial Ranking and Short-listing	November 3, 2021
Anticipated Interview Stage	November 12, 2021
Anticipated Final Ranking	November 18, 2021
Contract Negotiation Period	Thirty (30) calendar days
Anticipated Execution of Agreement	December 2021

The RFP timetable is tentative only and may be changed by EDC at any time. For greater clarity, business days means all days that EDC is open for business.

1.5 Submission Instructions

1.5.1 Submission of Proposals

Proposals must be submitted electronically through the bidding system at:

https://procurementoffice.bonfirehub.ca/opportunities/45274

Submissions by other methods will not be accepted.

In the event of any technical issues, proponents should contact the bidding system's technical support.

1.5.2 Proposals to Be Submitted on Time

Proposals must be finalized and fully uploaded in the bidding system on or before the Submission Deadline. The time of receipt of proposals shall be determined by the bidding system web clock. Late submissions will not be accepted by the bidding system and will be disqualified as late.

Proponents are cautioned that the timing of submission is based on when the proposal is received by the bidding system, not when a proposal is submitted by a proponent. As transmission can be delayed due to file transfer size, transmission speed, or other technical factors, proponents should plan to submit proposals well in advance of the Submission Deadline to avoid submitting late due to technical issues. Proponents submitting near the Submission Deadline do so at their own risk.

The bidding system will send a confirmation email to the proponent advising when the proposal was submitted successfully. If you do not receive a confirmation email, contact the bidding system's technical support immediately.

1.5.3 Proposals to Be Submitted in Prescribed Format

Proposal materials should be prepared and submitted in accordance with the instructions in the bidding system, including any maximum upload file size.

Documents should not be embedded within uploaded files, as the embedded files may not be accessible or evaluated.

1.5.4 Amendment of Proposals

Proponents may amend their proposals prior to the Submission Deadline. However, the proponent is solely responsible for ensuring that the amended proposal is received by the bidding system by the Submission Deadline.

1.5.5 Withdrawal of Proposals

At any time throughout the RFP process until the execution of a written agreement for provision of the Deliverables, a proponent may withdraw a submitted proposal. Prior to the Submission Deadline, proponents may withdraw a submitted proposal through the bidding system. To withdraw a proposal after the Submission Deadline, a notice of withdrawal must be sent to the RFP Contact and must be signed by an authorized representative of the proponent.

[End of Part 1]

PART 2 – EVALUATION, NEGOTIATION, AND AWARD

2.1 Stages of Evaluation and Negotiation

EDC will conduct the evaluation of proposals and negotiations in the following stages:

2.2 Stage I – Mandatory Submission Requirements

Stage I will consist of a review to determine which proposals comply with all of the mandatory submission requirements. If a proposal fails to satisfy all of the mandatory submission requirements, EDC will issue the proponent a rectification notice identifying the deficiencies and providing the proponent an opportunity to rectify the deficiencies. If the proponent fails to satisfy the mandatory submission requirements within the Rectification Period, its proposal will be rejected. The Rectification Period will begin to run from the date and time that EDC issues a rectification notice to the proponent. The mandatory submission requirements are set out in Section C of the RFP Particulars (Appendix B).

2.3 Stage II – Evaluation

Stage II will consist of the following two (2) sub-stages:

2.3.1 Mandatory Technical Requirements

EDC will review the proposals to determine whether the mandatory technical requirements as set out in Section D of the RFP Particulars (Appendix B) have been met. If a proposal fails to satisfy all of the mandatory technical requirements, EDC will issue the proponent a rectification notice identifying the deficiencies and providing the proponent an opportunity to rectify the deficiencies. The rectification process for these requirements may occur after any rectification process for mandatory submission requirements. Proposals that do not satisfy the mandatory technical requirements within the Rectification Period will be rejected.

2.3.2 Non-Price Rated Criteria

EDC will evaluate each qualified proposal on the basis of the non-price rated criteria as set out under Initial Evaluation Criteria in Section F of the RFP Particulars (Appendix B).

2.4 Stage III – Pricing

Stage III will consist of a scoring of the submitted pricing of each qualified proposal in accordance with the price evaluation method set out in Section G of the RFP Particulars (Appendix B). The evaluation of price will be undertaken after the evaluation of mandatory requirements and rated criteria has been completed.

In the event that a proponent's pricing appears to be abnormally low in relation to the Deliverables, EDC may require the proponent to provide a detailed explanation of the pricing information to account for the low level of price and confirm that all requirements in respect of the Deliverables have been taken into account. If the proponent is unable to satisfactorily account for the abnormally low pricing, EDC may reject the proposal. EDC may also reject any proposal that contains unbalanced pricing. Pricing may be considered unbalanced where nominal or significantly understated prices are proposed for some elements of the Deliverables and inflated prices are proposed for other elements of the Deliverables. Unbalanced pricing includes, but is

not limited to, “front-loaded” pricing which contains inflated pricing for Deliverables to be provided or completed at the beginning of the contract, offset by understated pricing for Deliverables to be provided or completed later in the contract.

2.5 Stage IV – Initial Ranking, Short-Listing, and Interview Stage

2.5.1 Initial Ranking of Proponents

After the completion of Stage III, all scores from Stage II and Stage III will be added together and the proponents will be initially ranked based on their total scores.

2.5.2 Short-Listing

EDC intends to short-list the top three (3) ranked proponents and invite the short-listed proponents to participate in an interview stage. If the score of the third-ranked proponent is greater than ten (10.0) points from the score of the second-ranked proponent, only the top two (2) ranked proponents will be invited to participate in the interview stage.

2.5.3 Interview Stage

The short-listed proponents will be invited to participate in an interview stage. The interview stage will be used by EDC to validate information contained in the short-listed proponent’s proposal. Based on the interview stage, evaluators may re-evaluate and re-score the non-price rated criteria. Further details regarding the Interview Stage will be provided via supplementary disclosures to the short-listed proponents with their notice of short-listing.

2.5.4 Final Ranking of Proponents

Following the interview stage, short-listed proponents will be assigned a final ranking using the same process set out above in Section 2.5.1 Initial Ranking of Proponents. The top-ranked proponent will receive a written invitation to enter into contract negotiations to finalize an agreement with EDC. In the event of a tie in the ranking of the top-ranked proponent, the selected proponent will be the proponent with the highest score on the non-price rated criteria.

2.6 Stage V – Contract Negotiations

2.6.1 Contract Negotiation Process

Any negotiations will be subject to the process rules contained in the Terms and Conditions of the RFP Process (Part 3) and will not constitute a legally binding offer to enter into a contract on the part of EDC or the proponent and there will be no legally binding relationship created with any proponent prior to the execution of a written agreement. The terms and conditions found in the Form of Agreement (Appendix A) are to form the basis for commencing negotiations between EDC and the selected proponent. Negotiations may include requests by EDC for supplementary information from the proponent to verify, clarify, or supplement the information provided in its proposal or to confirm the conclusions reached in the evaluation, and may include requests by EDC for improved pricing or performance terms from the proponent.

2.6.2 Time Period for Negotiations

EDC intends to conclude negotiations and finalize the agreement with the top-ranked proponent during the Contract Negotiation Period, commencing from the date EDC invites the top-ranked proponent to enter negotiations. A proponent invited to enter into direct contract negotiations should therefore be prepared to satisfy the pre-conditions of award listed in Section E of the RFP Particulars (Appendix B), provide requested information in a timely fashion, and conduct its negotiations expeditiously.

2.6.3 Failure to Enter into Agreement

If the pre-conditions of award listed in Section E of the RFP Particulars (Appendix B) are not satisfied or if the parties cannot conclude negotiations and finalize the agreement for the Deliverables within the Contract Negotiation Period, EDC may discontinue negotiations with the top-ranked proponent and may invite the next-best-ranked proponent to enter into negotiations. This process will continue until an agreement is finalized, until there are no more proponents remaining that are eligible for negotiations, or until EDC elects to cancel the RFP process.

2.6.4 Notification of Negotiation Status

Other proponents that may become eligible for contract negotiations may be notified at the commencement of the negotiation process with the top-ranked proponent.

[End of Part 2]

PART 3 – TERMS AND CONDITIONS OF THE RFP PROCESS

3.1 General Information and Instructions

3.1.1 Proponents to Follow Instructions

Proponents should structure their proposals in accordance with the instructions in this RFP. Where information is requested in this RFP, any response made in a proposal should reference the applicable section numbers of this RFP.

A proponent who submits conditions, options, variations, or contingent statements, either as part of its proposal or after receiving notice of selection, may be disqualified.

3.1.2 Proposals in English or French

All proposals are to be in English or French only.

3.1.3 No Incorporation by Reference

The entire content of the proponent's proposal should be submitted in a fixed format, and the content of websites or other external documents referred to in the proponent's proposal, but not attached, will not be considered to form part of its proposal.

3.1.4 Past Performance

In the evaluation process, EDC may consider the proponent's past performance or conduct on previous contracts with EDC or other institutions.

3.1.5 Information in RFP Only an Estimate

EDC and its advisers make no representation, warranty, or guarantee as to the accuracy of the information contained in this RFP or issued by way of addenda. Any quantities shown or data contained in this RFP or provided by way of addenda are estimates only and are for the sole purpose of indicating to proponents the general scale and scope of the Deliverables. It is the proponent's responsibility to obtain all the information necessary to prepare a proposal in response to this RFP.

3.1.6 Proponents to Bear Their Own Costs

The proponent will bear all costs associated with or incurred in the preparation and presentation of its proposal, including, if applicable, costs incurred for interviews or demonstrations.

3.1.7 Proposal to be Retained by EDC

EDC will not return the proposal or any accompanying documentation submitted by a proponent.

3.1.8 No Guarantee of Volume of Work or Exclusivity of Contract

EDC makes no guarantee of the value or volume of work to be assigned to the selected proponent. The agreement to be negotiated with the selected proponent will not be an exclusive contract for the provision of the described Deliverables. EDC may contract with others for goods

and services the same as or similar to the Deliverables or may obtain such goods and services internally.

3.2 Communication after Issuance of RFP

3.2.1 Proponents to Review RFP

Proponents should promptly examine all of the documents comprising this RFP and may direct questions or seek additional information in writing through the bidding system OR by email to the RFP Contact on or before the Deadline for Questions. No such communications are to be sent or initiated through any other means. EDC is under no obligation to provide additional information, and EDC is not responsible for any information provided by or obtained from any source other than the RFP Contact or the bidding system. It is the responsibility of the proponent to seek clarification from the RFP Contact on any matter it considers to be unclear. EDC is not responsible for any misunderstanding on the part of the proponent concerning this RFP or its process.

3.2.2 All New Information to Proponents by Way of Addenda

This RFP may be amended only by addendum in accordance with this section. If EDC, for any reason, determines that it is necessary to provide additional information relating to this RFP, such information will be communicated to all proponents by addendum. Each addendum forms an integral part of this RFP and may contain important information, including significant changes to this RFP. Proponents are responsible for obtaining all addenda issued by EDC.

3.2.3 Post-Deadline Addenda and Extension of Submission Deadline

If EDC determines that it is necessary to issue an addendum after the Deadline for Issuing Addenda, EDC may extend the Submission Deadline for a reasonable period of time.

3.2.4 Verify, Clarify, and Supplement

When evaluating proposals, EDC may request further information from the proponent or third parties in order to verify, clarify, or supplement the information provided in the proponent's proposal. EDC may revisit, re-evaluate, and rescore the proponent's response or ranking on the basis of any such information.

3.3 Notification and Debriefing

3.3.1 Notification to Other Proponents

Once an agreement is executed by EDC and a proponent, the other proponents may be notified directly in writing and will be notified by public posting of the outcome of the procurement process.

3.3.2 Debriefing

Proponents may request a debriefing after receipt of a notification of the outcome of the procurement process. All requests must be in writing to the RFP Contact and must be made within thirty (30) days of such notification. The RFP Contact will contact the proponent's representative to schedule the debriefing. Debriefings may occur in person at EDC's location or by way of conference call or other remote meeting format as prescribed by EDC.

3.4 Conflict of Interest and Prohibited Conduct

3.4.1 Conflict of Interest

For the purposes of this RFP, the term "Conflict of Interest" includes, but is not limited to, any situation or circumstance where:

(a) in relation to the RFP process, the proponent has an unfair advantage or engages in conduct, directly or indirectly, that may give it an unfair advantage, including, but not limited to:

  (i) having or having access to confidential information of EDC in the preparation of its proposal that is not available to other proponents;

  (ii) having been involved in the development of the RFP, including having provided advice or assistance in the development of the RFP;

  (iii) receiving advice or assistance in the preparation of its response from any individual or entity that was involved in the development of the RFP;

  (iv) communicating with any person with a view to influencing preferred treatment in the RFP process (including, but not limited to, the lobbying of decision-makers involved in the RFP process); or

  (v) engaging in conduct that compromises, or could be seen to compromise, the integrity of the open and competitive RFP process or render that process non-competitive or unfair; or

(b) in relation to the performance of its contractual obligations under a contract for the Deliverables, the proponent's other commitments, relationships, or financial interests:

  (i) could, or could be seen to, exercise an improper influence over the objective, unbiased, and impartial exercise of its independent judgement; or

  (ii) could, or could be seen to, compromise, impair, or be incompatible with the effective performance of its contractual obligations.

3.4.2 Disqualification for Conflict of Interest

EDC may disqualify a proponent for any conduct, situation, or circumstances, determined by EDC, in its sole and absolute discretion, to constitute a Conflict of Interest as defined above.

An existing supplier of EDC may be precluded from participating in the RFP process in instances where EDC has determined that the supplier has a competitive advantage that cannot be adequately addressed to mitigate against unfair advantage. This may include, without limitation, situations in which an existing supplier is in a position to create unnecessary barriers to competition through the manner in which it performs its existing contracts, or situations where the incumbent fails to provide the information within its control or otherwise engages in conduct obstructive to a fair competitive process.

3.4.3 Disqualification for Prohibited Conduct

EDC may disqualify a proponent, rescind an invitation to negotiate, or terminate a contract subsequently entered into if EDC determines that the proponent has engaged in any conduct prohibited by this RFP.

3.4.4 Prohibited Proponent Communications

Proponents must not engage in any communications that could constitute a Conflict of Interest and should take note of the Conflict of Interest declaration set out in the Submission Form (Appendix C).

3.4.5 Proponent Not to Communicate with Media

Proponents must not, at any time directly or indirectly, communicate with the media in relation to this RFP or any agreement entered into pursuant to this RFP without first obtaining the written permission of the RFP Contact.

3.4.6 No Lobbying

Proponents must not, in relation to this RFP or the evaluation and selection process, engage directly or indirectly in any form of political or other lobbying whatsoever to influence the selection of the selected proponent(s).

3.4.7 Illegal or Unethical Conduct

Proponents must not engage in any illegal business practices, including activities such as bid-rigging, price-fixing, bribery, fraud, coercion, or collusion. Proponents must not engage in any unethical conduct, including lobbying, as described above, or other inappropriate communications; offering gifts to any employees, officers, agents, elected or appointed officials, or other representatives of EDC; deceitfulness; submitting proposals containing misrepresentations or other misleading or inaccurate information; or any other conduct that compromises or may be seen to compromise the competitive process provided for in this RFP.

3.4.8 Supplier Suspension

EDC may suspend a supplier from participating in its procurement processes for prescribed time periods based on past performance or based on inappropriate conduct, including, but not limited to the following:

(a) illegal or unethical conduct as described above;

(b) the refusal of the supplier to honour its submitted pricing or other commitments;

(c) engaging in litigious conduct, bringing frivolous or vexatious claims in connection with EDC's procurement processes or contracts, or engaging in conduct obstructive to a fair competitive process; or

(d) any conduct, situation, or circumstance determined by EDC, in its sole and absolute discretion, to have constituted an undisclosed Conflict of Interest.

In advance of a decision to suspend a supplier, EDC will notify the supplier of the grounds for the suspension and the supplier will have an opportunity to respond within a timeframe stated in the notice. Any response received from the supplier within that timeframe will be considered by EDC in making its final decision.

3.5 Confidential Information

3.5.1 Confidential Information of EDC

All information provided by or obtained from EDC in any form in connection with this RFP either before or after the issuance of this RFP:

(a) is the sole property of EDC and must be treated as confidential;

(b) is not to be used for any purpose other than replying to this RFP and the performance of any subsequent contract for the Deliverables;

(c) must not be disclosed without prior written authorization from EDC; and

(d) must be returned by the proponent to EDC immediately upon the request of EDC.

3.5.2 Confidential Information of Proponent

A proponent should identify any information in its proposal or any accompanying documentation supplied in confidence for which confidentiality is to be maintained by EDC. The confidentiality of such information will be maintained by EDC, except as otherwise required by law or by order of a court or tribunal. Proponents are advised that their proposals will, as necessary, be disclosed, on a confidential basis, to advisers retained by EDC to advise or assist with the RFP process, including the evaluation of proposals. If a proponent has any questions about the collection and use of personal information pursuant to this RFP, questions are to be submitted to the RFP Contact.

3.6 Procurement Process Non-Binding

3.6.1 No Contract A and No Claims

This procurement process is not intended to create and will not create a formal, legally binding bidding process and will instead be governed by the law applicable to direct commercial negotiations. For greater certainty, and without limitation:

(a) this RFP will not give rise to any Contract-A-based tendering law duties or any other legal obligations arising out of any process contract or collateral contract; and

(b) neither the proponent nor EDC will have the right to make any claims (in contract, tort, or otherwise) against the other with respect to the award of a contract, failure to award a contract, or failure to honour a proposal submitted in response to this RFP.

3.6.2 No Contract until Execution of Written Agreement

This RFP process is intended to identify prospective suppliers for the purposes of negotiating potential agreements. No legal relationship or obligation regarding the procurement of any good or service will be created between the proponent and EDC by this RFP process until the

successful negotiation and execution of a written agreement for the acquisition of such goods and/or services.

3.6.3 Non-Binding Price Estimates

While the pricing information provided in proposals will be non-binding prior to the execution of a written agreement, such information will be assessed during the evaluation of the proposals and the ranking of the proponents. Any inaccurate, misleading, or incomplete information, including withdrawn or altered pricing, could adversely impact any such evaluation or ranking or the decision of EDC to enter into an agreement for the Deliverables.

3.6.4 Cancellation

EDC may cancel or amend the RFP process without liability at any time.

3.7 Governing Law and Interpretation

These Terms and Conditions of the RFP Process (Part 3):

(a) are intended to be interpreted broadly and independently (with no particular provision intended to limit the scope of any other provision);

(b) are non-exhaustive and will not be construed as intending to limit the pre-existing rights of the parties to engage in pre-contractual discussions in accordance with the common law governing direct commercial negotiations; and

(c) are to be governed by and construed in accordance with the laws of the province of Ontario and the federal laws of Canada applicable therein.

[End of Part 3]

APPENDIX A – FORM OF AGREEMENT

The Form of Agreement will be released via addendum prior to the Deadline for Addenda as stipulated in the RFP.

APPENDIX B – RFP PARTICULARS

A. THE DELIVERABLES

1. Background

For seventy-five (75) years, EDC has been dedicated to helping Canadian companies of all sizes succeed on the world stage. EDC is a financial Crown corporation that equips Canadian companies with the tools, trade knowledge, financing solutions, equity, insurance, and connections they need to grow their business with confidence. As international risk experts, EDC makes trade safer for Canadian companies. Underlying all of EDC's support is a commitment to sustainable and responsible business.

For additional information, please visit EDC's website at www.edc.ca.

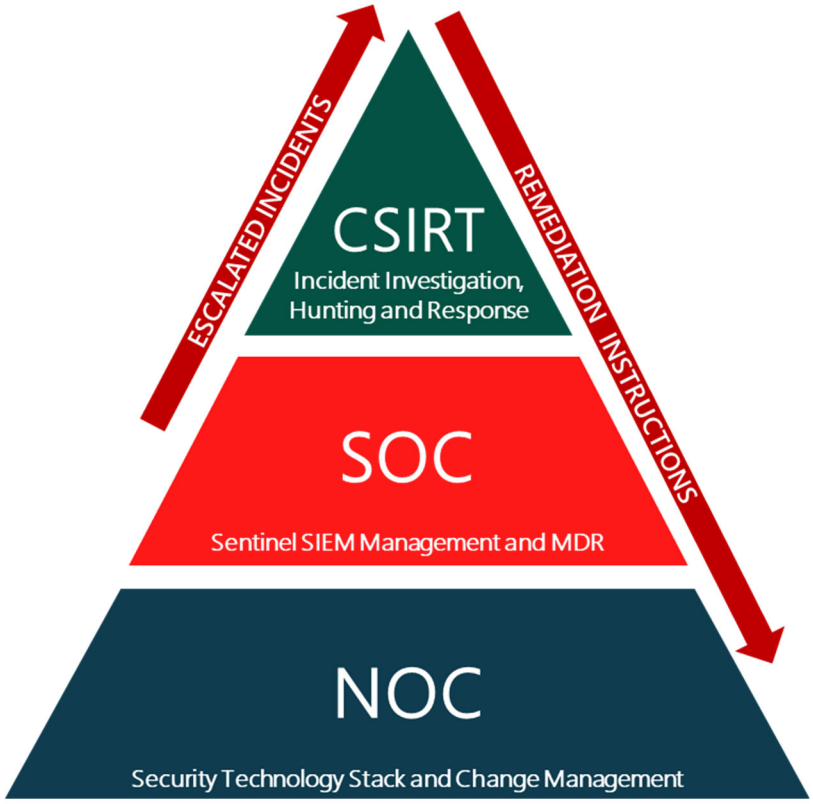
2. Engagement Overview

EDC's objective is to select a security operations center ("SOC") and managed detection and response ("MDR") provider that will be responsible for detecting intrusions, malware, and malicious activity in EDC's networks, including on-premises, cloud, and SaaS applications and platforms, while eliminating false positives and identifying real security threats, and assisting in rapid response to eliminate and mitigate those threats.

The provider will also be responsible for managing, monitoring, and maintaining EDC's Microsoft Azure Sentinel Instance, as well as working alongside EDC and its network operations teams to integrate new services and solutions into the security information and event management ("SIEM"). The provider will work in conjunction with EDC's security and operational teams to protect EDC's business.

3. Concept of Operations

EDC envisions that the SOC area of EDC's cybersecurity management structure (as depicted below) will be provided by the provider:



EDC's network operations centre ("NOC") is responsible for the day-to-day network operating and support activities, such as installing new products, machines, systems, and software, fixing and remediating vulnerabilities, and utilizing threat intel for proactive defense measures. EDC's computer security incident response team ("CSIRT") is the escalation point for additional investigation or triage.

EDC will make available to the provider 'read-only' access to systems, but will rely upon the provider to:

- design, suggest, and implement Sentinel workbooks to automate common remediation and defensive actions; and
- provide guidance to ensure the overall security program is operating at an optimal level.

Further, EDC will require the following services from the provider:

i. Threat Monitoring and Alerting

The provider must:

- monitor EDC's Microsoft Sentinel instance and existing on-premise environment (QRadar) for threats;
- alert the EDC CSIRT team when threats are discovered; and
- provide initial steps for remediation and eradication of the threat.

ii. Cybersecurity Advisory

The provider will assign a named senior cybersecurity advisor to analyse SOC service performance for EDC, and EDC-relevant geopolitical and industry threats, advisories, and general industry developments on a quarterly basis. The cybersecurity advisor will provide EDC with strategic and tactical advice for ongoing SOC and general cybersecurity improvements in a written report on a quarterly basis.

4. Requirements

i. Provider Information

The provider (which, for greater clarity, means the organization responsible for providing the Deliverables, not individuals working on the contract, except where expressly noted) must:

a) have a minimum of three (3) years experience in providing SOC services and a minimum of one (1) year of experience providing Sentinel SIEM-based SOC services;
b) have experience with engagements of similar size, scale, and complexity; experience in delivering services in Canada and working within the requirements of Canada's privacy and data laws are considered assets;
c) agree to EDC's right to perform SOC visits for audit, review, and compliance purposes;
d) have in place a business continuity plan ("BCP") in the event its SOC is unavailable;
e) have on staff a minimum of ten (10) SC-200 Microsoft Certified: Security Operations Analyst Associates with a minimum of one (1) year of experience;
f) provide resources that have a minimum of the Government of Canada's Enhanced Reliability security clearance, or equivalent as determined by EDC Security; for greater clarity, proponents should note that the requirements of such a security screening may include verification of personal data, educational and professional qualifications, employment history, and other similar checks;
g) have in place an internal cybersecurity controls framework implemented at its SOC facilities, such as NIST, ISO27000, SOC 2, SOC 3, CIS CSC, or PCI DSS;
h) inform EDC of any breaches in a timely fashion, including incidents affecting the provider or their key technology providers, where there is a possibility of impact on EDC services or EDC data.
i) inform EDC of any shared responsibility for breaches impacting EDC and whether the provider's liability insurance would provide EDC with compensation; and
j) provide core SOC monitoring and management and ensure that these are performed by full-time staff; for greater clarity, these SOC services cannot be outsourced to third parties.

Proponents should note that the above-noted requirements will be evaluated as detailed in Section F. Evaluation Criteria.

ii. SOC Services

The provider must provide Microsoft Azure Sentinel-based SOC and MDR services twenty-four (24) hours a day, seven (7) days a week, three hundred sixty-five (365) days a year. Further, the provider must operate its Sentinel SIEM SOC service in co-ordination with EDC's cybersecurity operations structure that includes EDC NOC (responsible for technology management and change management for incident mitigations) and EDC CSIRT (responsible to respond to SOC-escalated incidents and facilitate mitigations and remediations). The provider must ensure that all of their employees assigned to the EDC contract are aware of, understand, and adhere to

Canada's privacy laws (including, but not limited to, the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*")) to ensure the confidentiality of EDC's data.

Incidents escalated by the provider will be investigated by the EDC CSIRT who will in turn (and as needed) initiate the EDC change management process (change advisory board ("CAB")) that will engage EDC NOC to implement configuration changes as necessary to mitigate the incident. All incidents must be escalated via the provider's ticketing system, referencing and linking to the specific incident in Sentinel.

EDC desires to gradually increase the extent of automated mitigations utilizing Sentinel SOAR functions. The provider will be responsible for suggesting and implementing initial low-risk high-frequency automations, and progressively adding automations in line with global threats and EDC-specific incidents.

The EDC CSIRT will, from time to time, propose new playbooks, workbooks, and SOAR automations for the provider to implement.

Proponents should note that for the purposes of the RFP, the term "alerts" is used to reference the automatic alerts that are generated by Sentinel, while the term "incidents" is used to reference alerts that were triaged, determined to be true-positives, and are being escalated to EDC CSIRT for investigation/remediation.

The provider must provide details about workflows and processes of the event lifecycle, including how an event is described to a SOC analyst, how it is evaluated and triaged, what Sentinel mechanisms are used to capture relevant information to enrich the event, how SOAR orchestration may be invoked, how EDC CSIRT will be alerted to the event, and how the captured information will be shared with EDC CSIRT.

The provider must manage and operate EDC-owned Azure Sentinel SIEM/SOAR instance and integrate with the provider's Sentinel SIEM using Sentinel Lighthouse and in a manner that will ensure complete security of the EDC environment and is in isolation from the provider's other SOC customers.

The provider must be able to perform basic (Azure/M365-recommended) threat mitigation activities that were pre-approved by the EDC CSIRT in EDC's AD and M365 instances using a combination of Azure Lighthouse and the Azure AD B2B collaboration feature and in a manner that will ensure complete security of the EDC environment and is in isolation from the provider's other SOC customers.

The provider must provide EDC CSIRT with sufficient level of access that will allow EDC CSIRT to independently perform incident triage and threat hunting activities, while having access to the same information about incidents, threat intelligence feeds, and other relevant information and tools (including but not limited to Sentinel-native and external threat intelligence and threat hunting tools and services) as those that are available to the provider's SOC analysts.

The provider must acknowledge and follow a change management methodology for any changes to the SOC operating model or systems and services supporting the operating model. This includes changes to SIEM, SOAR, integrations with log sources, network devices, communications protocols, use cases, playbooks, workbooks, notebooks, or any other change that could affect the service. A change management methodology will also be used should any party discontinue the service for any reason.

The provider must at all times maintain active subscriptions to at least two (2) of the following commercial threat intelligence and dark web monitoring services:

- Anomali ThreatStream
- CrowdStrike
- Cybersixgill Darkfeed
- IBM X-Force Exchange
- Mandiant Advantage
- Palo Alto AutoFocus
- DigitalShadows
- Canadian Cyber Threat Exchange (“CCTX”)
- RecordedFuture.

Proponents should refer to vi. Deliverable Liquidated Damages Tables for further details.

The provider must at all times maintain subscriptions to at least one (1) open-source threat intelligence and dark web monitoring service, such as MISP, Alien Labs OTX, Anomali Limo, Mandiant Advantage Free, Palo Alto MineMeld, or VirusTotal VTAPI. Proponents should refer to vi. Deliverable Liquidated Damages Tables for further details.

The provider should maintain subscriptions to threat hunting enrichment services, such as HYAS Insight, ReversingLabs A1000, and RiskIQ PassiveTotal. For greater clarity, while this is not a requirement, EDC would prefer that the provider maintains subscriptions to threat hunting enrichment services.

The provider must utilize a catalogue of all EDC's technology and service providers and utilize the provider's and EDC's subscriptions to threat intelligence and dark web monitoring services to provide EDC with advisories of new vulnerabilities, third-party breaches, and active threats that are relevant to EDC technology stack vendors and service providers within a maximum of three (3) business days. The provider must work with EDC CSIRT to obtain and maintain a current list of technologies, vendors, and service providers.

iii. SIEM Services

The provider must provide, during the initial EDC onboarding process, project management, guidance, detailed documentation, and work with EDC or its vendors to configure EDC Sentinel SIEM to ingest identified vulnerabilities from EDC's existing threat and vulnerability management (“TVM”) platforms. The provider should note that the TVM solutions that EDC is using may be changed in the future.

The provider must work with EDC or its vendors to configure EDC Sentinel SIEM instance to ingest configuration management database (“CMDB”) asset inventory, systems' properties, and business criticality from EDC's future ServiceNow platform.

The provider must provide, during the initial EDC onboarding process, project management, guidance, detailed documentation, and work with EDC or its vendors to configure event forwarding from all security-relevant EDC existing and future on-premises servers, network, and security platforms into the managed Sentinel SIEM using any combination of direct connectors, collectors, native syslog, Common Event Format (“CEF”), Windows Management Instrumentation (“WMI”), Azure Monitor Agents, custom connectors, and representational state transfer (“REST”) API interfaces, as applicable to specific platforms.

The on-premises platforms that EDC is using may be changed from time to time, and the provider must work with EDC and its vendors to onboard new platforms into Sentinel SIEM and offboard the decommissioned platforms.

The provider must provide project management, guidance, detailed documentation, and work with EDC or its vendors to integrate EDC's Azure and Azure security services (such as Security Center and Microsoft 365 Defender) using Azure Lighthouse; and, if beneficial, using a separate log analytics workspace for security logs, into the provider's managed Sentinel SIEM in order to ingest security events and to provide SOC analysts with the minimum necessary roles and the ability to perform alert triage and pre-approved low-risk incident mitigations.

The provider must provide project management, guidance, detailed documentation, and work with EDC or its vendors to integrate EDC's Microsoft 365 workloads using a combination of Azure Lighthouse and the Azure AD B2B collaboration feature into the managed Sentinel SIEM, to ingest security events, and to provide SOC analysts with the minimum necessary roles and the ability to perform alert triage and pre-approved low-risk incident mitigations

The cloud services that EDC is using may be changed from time to time, and the provider must work with EDC and its vendors to onboard new cloud services into Sentinel SIEM and offboard the decommissioned cloud services.

The provider must provide project management, guidance, detailed documentation, and work with EDC or its vendors to configure event forwarding from all EDC existing SaaS service subscriptions into the managed Sentinel SIEM. The SaaS services that EDC is using may be changed from time to time, and the provider must work with EDC and its vendors to onboard new SaaS services into Sentinel SIEM and offboard the decommissioned SaaS services.

The provider must have the necessary expertise and, as necessary, utilize programming, scripting (such as Python and PowerShell) and other techniques for standard or custom integrations to ingest or export events for all existing and future EDC on-premises, cloud (Azure or other), and SaaS (Microsoft or other) security technologies and services into EDC Sentinel SIEM using syslog forwarding, APIs, cloud storage buckets, local event storage, log polling or streaming, Azure Log Analytics storage, and other methods as applicable.

EDC currently leverages an on-premises deployment of QRadar. The provider must, for the duration of SOC transition and onboarding period, and until all EDC assets have been fully and successfully onboarded into Sentinel, at a minimum, ingest alerts from the QRadar platform into the EDC Sentinel SIEM instance and use agreed upon escalation process to escalate these to the EDC CSIRT team.

iv. Alert Triage and SOAR Remediation

The provider's SOC analysts must utilize Sentinel use cases, notebooks, and playbooks to perform alert triage and the reduction of false positives for Sentinel SIEM-generated automatic detections and alerts. The triage should be done in correlation with EDC asset inventory to incorporate asset business risk ratings and actual vulnerabilities, along with global threat intelligence, and dark web monitoring.

The provider must develop new and review existing Sentinel SOAR playbook automations and make them available once every three (3) months.

The provider's SOC analysts must utilize read-only access to EDC's on-premises and cloud security technology consoles, including Azure Security Center and M365 Security Center, and other EDC appliance interfaces and SaaS portals to supplement SIEM event data and enhance SOC analysts' alert triage activities.

The provider's SOC analysts must generate incidents for escalation to EDC CSIRT. The incidents should be accompanied by extensive event and alert details and include a threat risk assessment based on asset risk rating (based on EDC information, such as the CMDB), known relevant vulnerabilities, and threat prevalence. The incidents should be accompanied with detailed mitigation and remediation guidance.

The provider should utilize their standard ticketing system and agreed-upon service level agreements ("SLA"s) and processes to escalate triaged alerts as tickets linking to the incident in Sentinel that is accompanied by all information collected during the triage by the SOC analysts.

v. Service Quality Management

The provider's contractual SLA commitment for the maximum time to respond to a Sentinel alert and start the triage process shall not exceed fifteen (15) minutes.

The provider's contractual SLA commitment for the maximum time to complete alert triage and to either dismiss as false positive, remediate it using SOAR automation, or escalate it as a fully documented incident to EDC CSIRT shall not exceed two (2) hours.

The provider's contractual SLA commitment for percentage of false-positive alerts that may be escalated to EDC CSIRT shall be no greater than five percent (5%).

a) Service Status and Performance Portal

EDC would prefer that the provider maintain and provide EDC with access to a service status and performance portal (secured with Azure AD SAML based single sign-on ("SSO") authentication and multi-factor authentication ("MFA")). At a minimum, the provider must provide EDC with a service status and performance portal report based on the live dashboards hosted on the portal that at a minimum include the following information:

1. Alerts

- Number of alerts autogenerated by Sentinel
- Number of incidents reported by EDC
- Number of incidents reported by EDC where the EDC-focused SOC analyst was not available within fifteen (15) minutes
- Number of incidents reported by EDC where the EDC-focused SOC analyst was not available within sixty (60) minutes
- Number of alerts or EDC-reported incidents that are pending start of triage for over fifteen (15) minutes
- Number of alerts or EDC-reported incidents that are pending incident escalation or dismissal as a false-positive for over two (2) hours
- Percentage of false positives

2. Incidents Escalated by SOC to EDC CSIRT

- Number of all open incidents
- Number of open critical incidents

- Number of incidents that were open for over twenty-four (24) hours
- Number of critical incidents that were open for over four (4) hours
- Number of concurrently open related and redundant incidents
- Breakdown of incidents by asset type, category, and severity

3. Change Requests ("CR"s) Submitted by or to be Actioned by SOC

- Number of open normal change requests
- Number of open critical change requests
- Number of normal CRs open for over two (2) weeks
- Number of emergency CRs open for over twenty-four (24) hours

4. SOC-Monitored Systems and Services

- Number of monitored systems and services
- Number of monitored systems and services not observed by SIEM for over twenty-four (24) hours
- Number of monitored systems and services with over twenty percent (20%) month-to-month change in number of received events

5. Breakdown of Attacks

- Attacks must be organized by attack type, such as, but not limited to:
- scanning IPs
- command-and-control IPs
- malicious emails
- malicious domains

b) Operational Reports

The provider must provide monthly operational reports on their performance and compliance with the SLAs that are specified in this RFP. The reports should be provided in a Microsoft Word format via the provider's customer portal every one (1) month, at least one (1) week prior to a one-hour (1-hour) operational meeting, where the report will be presented and discussed.

The reports must, at a minimum, address the monthly and previous twelve (12) months' trends of performance KPIs. The report must include the monthly values of at least ninety percent (90%) of all KPIs listed under the portal dashboard requirements above and the monthly values of at least ninety percent (90%) of the following:

- Number of true positive incidents
- Number and percentage of false positive incidents
- Number of Sentinel SOAR automation notebooks
- Breakdown of triggered Sentinel SOAR automations
- Breakdown of new Sentinel playbooks, workbooks, and notebooks created
- Critical observations, findings, and recommendations
- Number of decommissioned devices offboarded since last report
- Number of new devices onboarded since last report
- List of all Sentinel-triggered alerts, including the time when Sentinel triggered the alert, the time when a SOC analyst started triage, and the time when the alert was either mitigated by SOAR, or closed, or escalated to EDC CSIRT as an incident

The provider must regularly and at least once every three (3) months review previous alerts and incidents and develop or update Sentinel use cases, notebooks, and playbooks, and include the results in the next monthly report.

The provider must regularly, and at least once every three (3) months, review and assess global threat intelligence, and EDC, the Government of Canada, and the Cybersecurity and Infrastructure Agency (“CISA”) advisories of trending terrorist tactics, techniques, and procedures (“TTP”s), update its use cases, notebooks, and playbooks accordingly, and include the results in the next monthly report.

The provider must assign a named senior cybersecurity advisor who will regularly, at least once every three (3) months, analyze SOC service performance for EDC and EDC-relevant geopolitical and industry threats, advisories, and general industry developments. The senior cybersecurity advisor will provide EDC with strategic and tactical advice for ongoing SOC and general cybersecurity improvements provided to EDC quarterly in a written report delivered in Microsoft Word format. The senior cybersecurity advisor should facilitate a one-day (1-day) annual workshop, to ensure that the provider's Sentinel SOC processes, improvements, cybersecurity strategy, Microsoft and market developments, and the provider's innovation roadmap and updates are reviewed with the EDC team and that there is a continuing process of improvement for both parties.

The senior cybersecurity advisor must have at least three (3) years of experience in performing similar duties. In the event of a departure of this individual, EDC reserves the right to interview the proposed replacement candidate and/or ask for additional candidates to approve. The senior cybersecurity advisor may be a subcontractor to the provider.

The provider must make one (1) of their EDC-designated lead SOC analysts available to participate in a supporting role during the EDC annual incident response table-top and purple team exercises. EDC anticipates a total of four (4) hours per year dedicated to this exercise. In part, these exercises will be leveraged to improve EDC and SOC integration and readiness and to provide input for the annual workshop meetings.

The provider must assign a named SOC manager as the escalation point for tickets and SLA questions. The SOC manager must be available for critical escalations twenty-four (24) hours a day, seven (7) days a week, three hundred sixty-five (365) days a year within sixty (60) minutes at least fifty percent (50%) of the time and may not to exceed one hundred and twenty (120) minutes the rest of the time.

The provider must identify a named EDC-focused account manager as a single point of contact for EDC for contractual, SLA, and sales activities, and as an escalation point for service-related issues. The account manager must meet with EDC on a quarterly basis to review the provider's performance against the contract and other challenges, initiatives, service roadmaps, and innovations. The account manager should be available within seven (7) business days for meetings to facilitate contractual, SLA, and billing issues, changes to the provider's services or personnel, EDC change requests, and statements of work.

The provider must identify named cloud and on-premises cybersecurity specialists that understand cloud and on-premises cybersecurity technology software, hardware solutions, and should be available to EDC to assist in advisory or implementation capacity under a separate statement of work (“SOW”).

The provider must identify named SOC shift leads who must be available one hundred percent (100%) of the time on every shift (there will be shifts twenty-four (24) hours a day, seven (7) days a week, three hundred sixty-five (365) days a year). All SOC shift leads must posses at least three (3) years of SOC experience. When the SOC submits a CR to EDC CAB, one (1) of the provider's SOC shift leads or the SOC manager must attend EDC CAB meetings to address SOC-initiated change requests.

The provider must provide named EDC-focused SOC Analysts who must be available on every shift (there will be shifts twenty-four (24) hours a day, seven (7) days a week, three hundred sixty-five (365) days a year) within fifteen (15) minutes at least fifty percent (50%) of the time and not to exceed sixty (60) minutes the rest of the time. The EDC-focused SOC analysts must possess at least one (1) year experience.

The provider must have an innovation methodology that will ensure that Sentinel SOC services provided to EDC are not becoming irrelevant or obsolete over the term of the contract with EDC, and that the provider will be keeping up with the industry and with Microsoft Azure and Sentinel enhancements and will work with EDC to drive innovation for both parties. Areas of innovation will include, but may not be limited to:

- machine learning (“ML”) and artificial intelligence (“AI”), including and beyond Sentinel native ML and AI capabilities;
- research and development in the area of cybersecurity;
- ongoing SOAR optimization and XSOAR strategy, to reduce incident response dependency on EDC CSIRT and NOC;
- SOC threat hunting capabilities to reduce dependency on EDC CSIRT threat hunting; and
- integration of future Microsoft security stack enhancements to keep the pace with regular Microsoft enhancements.

vi. Deliverable Liquidated Damages Tables

The following tables detail the liquidated damages the provider will face if they fail to provide the following Deliverables as described above and in the table below by the due dates defined below. Proponents should note the enforcement of the below liquidated damages is at the discretion of EDC and that if the provider has failed to deliver two (2) or more of the below Deliverables, EDC reserves the right to terminate the contract for breach.

Requirement Reference	e) of i. Provider Information (Section 4. Requirements of A. Deliverables (Appendix B – RFP Particulars))
Deliverable Name	Provider Sentinel SOC Business Continuity Plan (“BCP”)
Format	Word document and PDF
Description	The BCP must include, at a minimum, the following components: 1. BCP Policy Statement 2. Emergency Notification and Crisis Impact 3. Crisis Notification Escalation Procedures

	4. Business Restoration Plan 5. Business Continuity Maintenance Plan 6. BCP Checklists 7. BCP Invocation Timeline a) Pre-Event Planning b) Initial Response Plan c) Business Resumption Plan 8. Manual Process List a) External Agreements and SLAs, if applicable 9. Risk Assessment 10. Alternate Site Requirements 11. Pandemic Business Continuity 12. Local Response Plan 13. BCP Testing Exercise Results
Frequency	Annually
Due Date	Initial Version: Sixty (60) business days after contract award Updated and re-issued on the anniversary date of contract award, or the next business day if the anniversary day falls on a weekend or statutory holiday
Liquidated Damages	Two thousand dollars ($2,000.00) a day for the first (1st) business day missed, and five hundred dollars ($500.00) per business day for every missed day thereafter

Requirement Reference	g) of i. Provider Information (Section 4. Requirements of A. Deliverables (Appendix B – RFP Particulars))
Deliverable Name	Provider Sentinel SOC Resource Report
Format	Word Document and PDF
Description	Table with the following rows: 1. Number of employees with federal security clearances who may work on the EDC contract 2. Number of employees without federal security clearances who may work on EDC contract 3. For provider employees assigned to the EDC contract, summary of the number of and types of criminal, financial, and background checks performed

	a) Number of checks passed b) Number of checks failed 4. Number of bilingual SOC analysts per shift, on average, available to work on the EDC contract
Frequency	Twice a year
Due Date	On contract award First (1st) working day of every sixth (6th) month thereafter, or the next business day if the anniversary day falls on a weekend or statutory holiday
Liquidated Damages	Five hundred dollars ($500) a day for the first (1st) day missed, and $100 per business day for every missed day thereafter

Requirement Reference	(h) of i. Experience and Qualifications (F. Rated Criteria (Appendix B – RFP Particulars))
Deliverable Name	Provider Sentinel SOC Attestations of Compliance
Format	Word Document and PDF
Description	Attestations of Compliance (“AOC”) may include SOC2 Type 2 Reports, PCI Report of Compliance signed by a Qualified Security Assessor, or ISO certification document
Frequency	Annually
Due Date	With RFP Response Anniversary date of contract award, or the next business day if the anniversary day falls on a weekend or statutory holiday
Liquidated Damages	Post-contract award, five hundred dollars ($500.00) a day for the first (1st) day missed, and one hundred dollars ($100.00) per business day for every missed day thereafter

Requirement Reference	ii. SOC Services (4. Requirements of Section A. Deliverables (Appendix B – RFP Particulars))
Deliverable Name	Provider Sentinel SOC Change Management Process
Format	Word Document and PDF
Description	ITIL-driven change advisory and review process document

Frequency	Annually on the anniversary day of the contract and within thirty (30) days after being updated by the provider Regular changes must be tracked through the monthly report
Due Date	On contract Award and annually on the anniversary date of the contract award, or the next business day if the anniversary day falls on a weekend or statutory holiday
Liquidated Damages	Five hundred dollars ($500.00) a day for the first (1st) day missed, and one hundred dollars ($100.00) per business day for every missed day thereafter

Requirement Reference	ii. SOC Services (4. Requirements of Section A. Deliverables (Appendix B – RFP Particulars))
Deliverable Name	Provider Sentinel SOC Subscription Summary Report
Format	Word Document & PDF
Description	Table with the following rows: 1. Name of at least two (2) commercial threat intelligence and dark web monitoring services 2. Name of at least one (1) open-source threat intelligence and dark web monitoring service 3. Name of subscriptions to any threat hunting enrichment services And the following columns: 1. Subscription start date 2. Subscription end date
Frequency	Quarterly
Due Date	On contract award First (1st) day of every third (3rd) month thereafter, or the next business day if the anniversary day falls on a weekend or statutory holiday
Liquidated Damages	One thousand five hundred dollars ($1,500.00) a day for the first (1st) day missed, and five hundred dollars ($500.00) per business day for every missed day thereafter

Requirement Reference	v. Service Quality Management (4. Requirements of Section A. Deliverables (Appendix B – RFP Particulars))
Deliverable Name	Sentinel SOC Monthly Operational Report and Meeting
Format	Word document and PDF
Description	The report must include the monthly values and cover at least ninety percent (90%) of the following KPI's: 1. Alerts: a) Number of alerts autogenerated by Sentinel b) Number of incidents reported by EDC • Number of incidents reported by EDC where the EDC-focused SOC analyst was not available within fifteen (15) minutes • Number of incidents reported by EDC where the EDC-focused SOC analyst was not available within sixty (60) minutes c) Number of alerts or EDC-reported incidents that are pending start of triage for over fifteen (15) minutes d) Number of alerts or EDC-reported incidents that are pending incident escalation or dismissal as a false-positive for over two (2) hours e) Percentage of false positives 2. Incidents escalated by SOC to EDC CSIRT: a) Number of all open incidents b) Number of open critical incidents c) Number of incidents that were open for over twenty-four (24) hours d) Number of critical incidents that were open for over four (4) hours e) Number of concurrently open related and redundant incidents f) Breakdown of incidents by asset type, category, and severity 3. Change requests submitted by or to be actioned by SOC: a) Number of open normal CRs b) Number of open critical CRs

	c) Number of normal CRs open for over two (2) weeks d) Number of emergency CRs open for over twenty-four (24) hours 4. SOC-monitored systems and services: a) Number of monitored systems and services b) Number of monitored systems and services not observed by SIEM for over twenty-four (24) hours c) Number of monitored systems and services with over twenty percent (20%) month-to-month change in number of received events d) Number of events ingested by Sentinel 5. A breakdown of attacks broken down by attack types, such as, but not limited to: a) Scanning IPs b) Command-and-control IPs c) Malicious emails d) Malicious domains 6. Number of true positive incidents 7. Number and percentage of false positive incidents 8. Number of Sentinel SOAR automation notebooks 9. Breakdown of triggered Sentinel SOAR automations 10. Breakdown of new Sentinel playbooks, workbooks, and notebooks created 11. Critical observations, findings, and recommendations 12. Number of decommissioned devices offboarded since last report 13. Number of new devices onboarded since last report 14. List of all Sentinel-triggered alerts, including the time when Sentinel triggered the alert, the time when a SOC analyst started triage, and the time when the alert was either mitigated by SOAR, closed, or escalated to EDC CSIRT as an incident
Frequency	Monthly
Due Date	The report is to be delivered within five (5) business days from the beginning of each month

	The operational meeting is to be held at least two (2) business days after delivery of the report and no later than ten (10) business days from the beginning of each month
Liquidated Damages	Two thousand dollars ($2,000.00) a day for the first (1st) business day missed, and five hundred dollars ($500.00) per business day for every missed day thereafter

B. MATERIAL DISCLOSURES

1. Expertise

The provider must be experts in the following products:

- Microsoft Azure
- Azure Sentinel

2. Current Performance Specifications

- The average IBM QRadar logs per month are approximately one billion (1,000,000,000) events.
- The average events per second are between eleven thousand (11,000) and twelve thousand (12,000).

3. Technologies for Integration

Currently, EDC has the following technologies that must be integrated into Sentinel by the provider, who will be given limited access to these platforms to support triage activities. It is expected that some of these platforms will change over the span of the agreement and the provider must have the proficiency and flexibility to integrate these and future platforms.

Product	Quantity
BlueCat servers	4
Cisco AMP	1
Cisco ASA Firewalls	5
Cisco IronPort	4
Cisco Network switches	12
Cisco Umbrella	1
Cisco VPN gateways	4
Cisco Wireless controllers	2
Cisco WSA	5
Citrix WAF	4
CyberArk	4
FireEye Threat Intelligence	1

Product	Quantity
ForeScout NAC	4
Fortigate Firewalls	27
Fortigate VPN gateways	4
Gigamon TAPS	1
IBM X-Force Vulnerability Scanner	7
Linux Servers	20
LoginTC 2FA	2
Microsoft 365	1
Microsoft Active Directory servers	12
Microsoft Azure AD	1
Microsoft Azure Cloud	1
Microsoft Azure Defender ATP	1
Microsoft Azure Security Center	1
Microsoft Azure Sentinel	1
Microsoft WAF	3
Microsoft Windows Servers	125
One Identity Syslog	2
Progress Software MOVEit Cloud	1
Quest Change Auditor	1
ServiceNow	1
Symantec Endpoint Protection	2
Tenable Nessus	12
Tripwire Enterprise	2
Tripwire Expert OPS	1
TOTAL	**280**

4. Timetable of Knowledge Transfer

The provider is expected to start knowledge transfer activities no later than January 3, 2022. Further, the provider is expected to complete the knowledge transfer and assume the SOC and MDR responsibilities no later than April 1, 2022.

5. Out of Scope

As the provider will be leveraging EDC's Sentinel instance, any storage, traffic, and processing fees are the responsibility of EDC and are outside of the scope of this RFP.

C. MANDATORY SUBMISSION REQUIREMENTS

1. Submission Form (Appendix C)

Each proposal must include a Submission Form (Appendix C) completed and signed by an authorized representative of the proponent.

2. Pricing

Each proposal must include pricing information that complies with the instructions set out below in Section G of this Appendix B.

D. MANDATORY TECHNICAL REQUIREMENTS

N/A

E. PRE-CONDITIONS OF AWARD

1. Confirmation of Commercial General Liability Coverage

The selected proponent shall provide confirmation of, and maintain during the term of the Agreement, commercial general liability insurance coverage to a limit of not less than two million dollars ($2,000,000.00) per occurrence for bodily injury, death, and damage to property, including loss of use thereof. Such insurance coverage shall be in the name of the selected proponent and shall name EDC as an additional insured thereunder. The policy must include a cross-liability and severability of interest clause. Failure to provide confirmation will result in the disqualification of the proponent from the RFP process.

2. Confirmation of Workplace Safety and Insurance Board Coverage

The selected proponent must provide confirmation of Workplace Safety and Insurance Board coverage prior to the award of the contract. Failure to provide confirmation will result in the disqualification of the proponent from the RFP process.

3. Due Diligence Questionnaire

The selected proponent must complete and pass a Due Diligence Questionnaire, which will be released via addendum prior to the Submission Deadline as specified in the RFP.

F. EVALUATION CRITERIA

The following sections set out the categories, weightings, and descriptions of the evaluation criteria for both stages of the RFP. Proponents who do not meet a minimum threshold score for a category will not proceed to the next stage of the evaluation process.

1. Evaluation Criteria

The following categories, weightings, and descriptions will be used in the initial evaluation of rated criteria during Stage II of the evaluation process (Evaluations), described in Part 2 of this RFP. These criteria apply to initial proposals by all proponents.

Non-Price Rated Criteria Category	Weighting	Minimum Threshold
i. Experience and Qualifications	25 points	12.5 points out of 25 points
ii. SOC Services	12 points	6.0 points out of 12 points
iii. SIEM Services	5 points	2.5 points out of 5 points
iv. Alert Triage Services	5 points	2.5 points out of 5 points
v. Service Quality Management	28 points	14.0 points out of 28 points
Pricing (see Section G below)	**25 points**	**N/A**
Total Points	**100 points**	**N/A**

i. Experience and Qualifications – 25 points

Proponents should provide the following in their proposals:

(a) a description of three (3) project examples, where services of similar scope, size and complexity were provided within the last (3) years, for EDC to use as references for the proponent (1 point per project example for a total of three (3) points). The project examples provided must meet the following minimum criteria:

- Sentinel SIEM-based SOC client for at least one (1) year; and
- client staff of at least two thousand (2,000).

Project examples provided that do not meet the minimum criteria will receive a score of zero (0) points for that project example. Proponents should further note that project examples provided where the client organization's head office is located in Canada will receive an additional half point (0.5 points) per project example, as experience working with other Canadian institutions with similar privacy and security restrictions is an asset. For greater clarity, project examples that include a client organization head office located in Canada may receive a total of one and a half points (1.5) per project example.

Proponents should provide the following information for each project example:

- a description of services provided, including the number of client staff for the project;
- contract start date and end date, including Sentinel SIEM-based SOC duration;
- client organization name;
- client organization head office location; and
- client contact name and email address.

Note: The client contact provided for each of the project examples will be contacted and provided with Form 1 – Reference Validation, which has been provided with the RFP for reference purposes only. Proponents are responsible for ensuring the availability and willingness of the client contact to provide a reference. No points are assigned to the reference check and validation process; however, responses from the client contact will be considered in the scoring of the relevant criteria set out above. Form 1 – Reference Validation will be released via addendum by the Deadline for Addenda as stipulated in the RFP.

(b) indicate the organization's experience, expressed in years and months, in providing SOC services. Proponents will receive points as follows:

1. proponent has been providing SOC services for less than three (3) years = 0.5 points;
2. proponent has been providing SOC services for three (3) years to less than five (5) years = 1 point;
3. proponent has been providing SOC services for five (5) years to less than ten (10) years = 2 points; or
4. proponent has been providing SOC services for ten (10) years or more = 3 points;

(c) indicate the organization's experience, expressed in years and months, in providing Sentinel SIEM-based SOC services. Proponents will receive points as follows:

1. proponent has been offering Sentinel SIEM-based SOC services for less than one (1) year = 0.5 points; or
2. proponent has been offering Sentinel SIEM-based SOC services for one (1) year or more = 2 points;

(d) indicate the organization's number of current Sentinel SIEM SOC customers. Proponents will be awarded points as follows:

1. proponent has less than ten (10) Sentinel SIEM SOC customers = 0 points;
2. proponent has at least ten (10) but no more than twenty (20) Sentinel SIEM SOC customers = 0.5 points;
3. proponent has at least twenty-one (21) but no more than fifty (50) Sentinel SIEM SOC customers = 1 point;
4. proponent has at least fifty-one (51) but no more than one hundred (100) Sentinel SIEM SOC customers = 1.5 points; or
5. proponent has more than one hundred (100) Sentinel SIEM SOC customers = 2 points;

(e) the total count of systems monitored by Sentinel SIEM SOC. The count should exclude any monitored user endpoints. The count should include the combined number of monitored Azure and other cloud subscriptions, on-premises appliances and servers, and SaaS systems and services. Proponents will be awarded points as follows:

1. proponent has less than five thousand (5,000) Sentinel SIEM monitored systems = 0 points;
2. proponent has at least five thousand (5,000) but no more than ten thousand (10,000) Sentinel SIEM monitored systems = 0.5 points;
3. proponent has at least ten thousand (10,000) but no more than twenty-five thousand (25,000) Sentinel SIEM monitored systems = 1 point;
4. proponent has at least twenty-five thousand (25,000) but no more than fifty thousand (50,000) Sentinel SIEM monitored systems = 1.5 points; or
5. proponent has more than fifty thousand (50,000) Sentinel SIEM monitored systems = 2 points;

(f) a list of the named resources who will perform the role of Sentinel SIEM SOC analysts and their high-level curricula vitae that demonstrate their certifications and experience in providing the Deliverables. Further, the response provided should clearly indicate which analysts, if any, are bilingual (English and French). Proponents should refer to the Deliverables for a list of the requirements for proposed Sentinel SIEM SOC analysts. Proponents should further note that EDC recognizes that there may be an adjustment in

the availability of the named Sentinel SIEM SOC analysts – proponents should provide a list of named resources that are representative of the proponent's proposed approach to managing the Deliverables. For each analyst that meets or exceeds the requirements listed, a quarter of a point (0.25 points) will be awarded up to a maximum of two and a half (2.5) points for this criterion;

(g) describe internal cybersecurity controls framework implemented at the Sentinel SOC facilities, such as SOC 2, SOC 3, CIS CSC, or PCI DSS for any Sentinel SOC facilities (1 point);

(h) include valid Attestations of Compliance ("AOC") from auditors. The proponent will be rated higher for a greater number of different types of AOCs. Examples of acceptable AOCs include, but may not be limited to, PCI Report on Compliance, SOC2 Type 2, and ISO 27002. The AOCs will be counted as one (1) when the same type of audit was performed across the proponent's multiple Sentinel SOC facilities. Proponents will be rated higher for additional certification or validations. Proponents will be scored based on the following:

1. proponent has no AOCs = 0 points;
2. proponent has one (1) AOC = 1 point;
3. proponent has two (2) AOCs = 2 points; or
4. proponent has three (3) or more AOCs = 3 points;

(i) a description of any material cybersecurity incidents within the last two (2) years. Proponents should identify the categories of cybersecurity incidents that have occurred in the last two (2) years and the number of each incident per category. Further, proponents should note whether or not there was any material impact to the proponent or the client, whether or not there was any regulatory or legal action against the proponent or against the client as a result of the breach, and how the incident was mitigated. Proponents should note that all information regarding incidents must be anonymized. Proponents without any material breaches will receive full points (1 point); proponents that experienced a material cybersecurity incident but can provide a narrative proving the management of such an incident was robust and effective will receive 0.5 points); and

(j) a detailed curriculum vitae of the proposed individuals acting in each of the following roles as further described in the Deliverables (v. Service Quality Management of Section 4. Requirements) (1 point per role for a total of 4 points):

1. Senior Cybersecurity Advisor (1 point);
2. Senior Advisor (1 point);
3. SOC Manager (1 point); and
4. Account Executive (1 point).

ii. SOC Services – 12 points

Proponents should provide the following in their proposals:

(a) describe the workflows and processes of the event lifecycle, including how an event is described to a SOC analyst, how it is evaluated and triaged, what Sentinel mechanisms are used to capture relevant information to enrich the event, how SOAR orchestration may

be invoked, how EDC CSIRT will be alerted to the event, and how the captured information will be shared with EDC CSIRT (2 points);

(b) a listing of any active subscriptions to commercial threat intelligence and dark web monitoring services. Proponents should refer to the Deliverables (ii. SOC Services of Section 4. Requirements) for a listing of preferred subscription providers. Proponents will receive points as follows:

1. proponent has zero (0) or one (1) active subscriptions to commercial global threat intelligence and dark web monitoring services = 0 points;
2. proponent has two (2) active subscriptions to commercial global threat intelligence and dark web monitoring services = 0.5 points;
3. proponent has three (3) active subscriptions to commercial global threat intelligence and dark web monitoring services = 1 point; or
4. proponent has four (4) or more active subscriptions to commercial global threat intelligence and dark web monitoring services = 1.5 points;

(c) a listing of any active subscriptions to open-source threat intelligence and dark web monitoring services. Proponents should refer to the Deliverables (ii. SOC Services of Section 4. Requirements) for a listing of preferred subscription providers. Proponents will receive points as follows:

1. proponent has zero (0) or one (1) active subscriptions to open-source threat intelligence and dark web monitoring services = 0 points;
2. proponent has two (2) active subscriptions to open-source threat intelligence and dark web monitoring services = 0.5 points;
3. proponent has three (3) active subscriptions to open-source threat intelligence and dark web monitoring services = 1 point; or
4. proponent has four (4) or more active subscriptions to open-source threat intelligence and dark web monitoring services = 1.5 points;

(d) a listing of any active subscriptions to threat hunting enrichment services. Proponents should refer to the Deliverables (ii. SOC Services of Section 4. Requirements) for a listing of preferred subscription providers. Proponents will receive points as follows:

1. proponent has zero (0) active subscriptions to threat hunting enrichment services = 0 points; or
2. proponent has one (1) or more subscriptions to threat hunting enrichment services = 1 point;

(e) a description of the proposed approach to working with EDC CSIRT to obtain and maintain a current list of technologies, vendors, and service providers, and to provide advisories of new vulnerabilities, third-party breaches, and active threats that are relevant to EDC technology stack vendors and service providers (2 points);

(f) describe in detail the proposed method of access to EDC Sentinel instances and how the proponent will guarantee complete security and isolation between proponent clients, while enabling the SOC analysts and EDC's IT teams to access the same information in Sentinel (1 point);

(g) describe in detail the proposed method of access to EDC's Azure Sentinel Instance and the protocols used to guarantee the complete security and isolation between the proponent's clients (2 points); and

(h) describe and provide detailed screenshots of how EDC CSIRT will have access to the Sentinel instance, alert details, and all embedded tools and threat intelligence data (1 point).

iii. SIEM Services – 5 points

Proponents should provide the following in their proposals:

(a) a description of the proposed process for, and sharing of responsibilities, including a sample of detailed Sentinel onboarding instructions for at least three (3) of EDC's technology platforms listed in 3. Technologies for Integration (B. Material Disclosures of Appendix B) (1 point for each sample for a total of 3 points); and

(b) describe the proposed approach to leveraging EDC's on-premises deployment of QRadar, including, but not limited to, ingesting alerts from the QRadar platform into the EDC Sentinel SIEM instance, and use agreed upon escalation process to escalate these to the EDC CSIRT team. Proponents should note in their response if they are able to fully manage the QRadar software, including alert triage, as they will score higher for their ability to do so (2 points).

iv. Alert Triage and SOAR Remediation – 5 points

Proponents should provide the following in their proposals:

(a) a description of the typical frequency for developing new automations, and the proposed approach for making them available to EDC. Proponents should note that the minimum required, as stated in the Deliverables (iv. Alert Triage and SOAR Remediation of Section 4. Requirements) is once every three (3) months and that proponents will score higher for more frequently proposed updates (2 points);

(b) a description of how the proponent will generate incidents for escalation to EDC CSIRT in accordance with Deliverables (iv. Alert Triage and SOAR Remediation of Section 4. Requirements), including four (4) samples of incident documentation (0.5 points per sample for a total of 2 points); and

(c) a description of any other methods, besides the ticketing system (for example, email, call centre, or the like), that will be available to EDC for incident reporting purposes (1 point).

v. Service Quality Management – 28 points

Proponents should provide the following in their proposals:

(a) provide six (6) detailed screenshots of different views of the live customer dashboard (not Azure or Sentinel dashboards) that will be utilized to interact with EDC (0.5 points per screenshot for a total of 3 points);

(b) a description of the proposed approach to Sentinel SIEM generated automatic alerts being received by the SOC analyst and the SOC analyst initiating a triage alert. Proponents should note the requirement for maximum time allowed as noted in the Deliverables (v. Service Quality Management of Section 4. Requirements), and further note that proponents who provide for faster guaranteed response time will receive a higher score (3 points);

(c) provide the actual average over the last twelve (12) months across all clients of response time from Sentinel SIEM-generated automatic alert to a SOC analyst initiating alert triage. Proponents will be awarded points based on the following:

1. proponent's actual average response time from alert to initiating alert triage is more than fifteen (15) minutes = 0 points;
2. proponent's actual average response time from alert to initiating alert triage is between fifteen (15) minutes and more than ten (10) minutes = 0.5 points;
3. proponent's actual average response time from alert to initiating alert triage is between ten (10) minutes and more than five (5) minutes = 1 point; or
4. proponent's actual average response time from alert to initiating alert triage is five minutes or less = 3 points;

(d) a description of its proposed approach for integration with EDC's security operations teams, list any specific requirements for EDC IT, and define any SLA dependencies on EDC CAB, NOC, and CSIRT teams (2 points);

(e) provide the actual average last twelve (12) months' performance across all clients for the time it took to complete alert triage and, if determined to be a true positive, escalate to the client's IT. Proponents will be awarded points based on the following:

1. proponent's actual response time as described above was more than twenty percent (20.0%) higher than the proposed response time under (c) above = 0 points;
2. proponent's actual response time as described above was between twenty percent (20.0%) and more than fifteen percent (15.0%) higher than the proposed response time under (c) above = 0.5 points;
3. proponent's actual response time as described above was between fifteen percent (15.0%) and more than ten percent (10.0%) higher than the proposed response time under (c) above = 1 point;
4. proponent's actual response time as described above was between ten percent (10.0%) and more than five percent (5.0%) higher than the proposed response time under (c) above = 1.5 points; or
5. proponent's actual response time as described above was five percent (5.0%) or less than the proposed response time under (c) above = 3 points;

(f) a proposed commitment for the maximum percentage of false-positive alerts that may be escalated to EDC CSIRT. Proponents will be awarded points based on the following:

1. proponent's proposed percentage of false-positive alerts is greater than five percent (5%) = 0 points;
2. proponent's proposed percentage of false-positive alerts is between five percent (5%) and more than two percent (2%) = 0.5 points;

3. proponent's proposed percentage of false-positive alerts is between two percent (2%) and more than zero percent (0%) = 1 point; or
4. proponent's proposed percentage of false-positive alerts is zero percent (0%) = 2 points;

(g) provide the actual average last twelve (12) months performance across all clients for the percentage of false-positive alerts that have been escalated to client IT. Proponents will be awarded points based on the following:

1. proponent's actual average number of false positives, as described above, was more than twenty percent (20.0%) higher than the proposed percentage of false-positive alerts under (f) above = 0 points;
2. proponent's actual average number of false positives, as described above, was between twenty percent (20.0%) and more than fifteen percent (15.0%) higher than the proposed percentage of false-positive alerts under (f) above = 0.5 points;
3. proponent's actual average number of false positives, as described above, was between fifteen percent (15.0%) and more than ten percent (10.0%) higher than the proposed percentage of false-positive alerts under (f) above = 1 point;
4. proponent's actual average number of false positives, as described above, was between ten percent (10.0%) and more than five percent (5.0%) higher than the proposed percentage of false-positive alerts under (f) above = 1.5 points; or
5. proponent's actual average number of false positives, as described above, was five percent (5.0%) or less than the proposed percentage of false-positive alerts under (f) above = 3 points;

(h) a description of the proposed approach to reviewing previous alerts and incidents, developing or updating Sentinel use cases, notebooks and playbooks, and including the results in a report to EDC (2 points);

(i) a description of the proposed approach to developing or updating Sentinel use cases, notebooks, and playbooks based on global threat intelligence, EDC and Government of Canada, and CISA advisories of trending TTPs, updating the proponent's use cases, notebooks, and playbooks accordingly, and including the results in the next monthly report (2 points);

(j) a description of the proposed approach to reviewing past incidents to identify recurring patterns of simple and repetitive incidents that are candidates for SOAR automation and including these in the monthly operations report (2 points); and

(k) a description of the proposed process for collaboration with EDC CSIRT and EDC NOC teams and how responsibilities would be shared with EDC in the development, recommendation, and implementation of Sentinel SOAR workbooks for automated low-risk migration of routine incidents through integrations with EDC on-premises and cloud security platforms and services (3 points).

G. PRICE EVALUATION METHOD

Pricing is worth twenty-five (25) points of the total score. Points for pricing will be allocated as follows:

i. Committed Pricing for Requirements – 20 points (80% of total pricing points)
ii. Hourly Rates for Resources – 5 points (20% of total pricing points)

Pricing will be scored based on a relative pricing formula using the rates set out in the pricing form. Each proponent will receive a percentage of the total possible points allocated to price, as defined in Required Pricing Information, which will be calculated in accordance with the following formula:

$$lowest\ price \div proponent's\ price\ \times\ weighting = proponent's\ pricing\ points$$

Instructions on How to Provide Pricing

(a) Proponents should submit their pricing information by completing the attached pricing form and including it in their proposals.

(b) Rates must be provided in Canadian funds, inclusive of all applicable duties and taxes except for HST, which should be itemized separately.

(c) Unless otherwise indicated in the requested pricing information, rates quoted by the proponent must be all-inclusive and must include all labour and material costs, all travel and carriage costs, all insurance costs, all costs of delivery, all costs of installation and set-up, including any pre-delivery inspection charges, and all other overhead, including any fees or other charges required by law.

Required Pricing Information

i. Committed Pricing for Requirements – 20 points

1. Non-Recurring Charges ("NRC") – Initial Set-Up

Initial one-time (1-time) set-up cost, including the configuration and integration of EDC's existing asset inventory list of two hundred eighty (280) assets (Section 3. Technologies for Integration of B. Material Disclosures), including on-premises, cloud, and SaaS assets, into Sentinel within six (6) months of contract signing.

Proposed Initial NRC Price	**$**

2. Monthly Recurring Charges ("MRC") – Base Assets

Provide the MRC for ongoing monitoring services for all assets as defined in the Deliverables (Appendix B) for Year 1. For the purposes of the evaluation of pricing only, proponents should assume a volume of two hundred eighty (280) assets, as defined in Section 3. Technologies for Integration (B. Material Disclosures). Proponents should further note that the MRC will increase for Years 2 to 3, and the optional terms (Years 4 and 5), if applicable, annually by the Government of Canada consumer price index rate that is current at that time.

Year	**Proposed Annual MRC (280 Assets)**
Year 1	**$**

3. Expansion of Services NRC

To account for EDC's anticipated growth, provide one-time setup fees that will apply uniformly to all additional EDC assets beyond the initial two hundred eighty (280) devices. For greater clarity, provide the per asset initial set-up fee for the following asset volume tiers for each type of asset, which will apply to all assets of the same type onboarded in that volume tier. The Column Totals will be calculated by adding all of the volume tier NRC for each of the asset types and the Total Expansion NRC Price will be the sum of all the Column Totals. Proponents should note that the Total Expansion NRC Price will be used for scoring purposes only.

Volume Tier	**REST API (Standard Sentinel Integration) Proposed Price**	**REST API (Custom Integration) Proposed Price**	**CEF Over Syslog Proposed Price**
281 to 300 assets			
301 to 350 assets			
351 to 400 assets			
401 to 450 assets			
451 to 500 assets			
501 or more assets			
COLUMN TOTALS:	**$**	**$**	**$**
TOTAL EXPANSION NRC PRICE (sum of all column totals from row above)		**$**	

4. Expansion of Services MRC

To account for EDC's anticipated growth, provide the MRC that will apply uniformly to all additional EDC assets beyond the initial two hundred eighty (280) devices. For greater clarity, provide the MRC that will be applied to all assets monitored during the months where the number of assets are within that volume tier. Proponents should note that as EDC is responsible for Azure Sentinel consumption fees, the provider should be flexible to reduce the number of monitored assets with no penalties. For greater clarity, proponents should assume a minimum of two hundred eighty (280) assets for pricing purposes only. The Total Volume MRC will be calculated by adding all of the Proposed MRC Prices and will only be used for scoring purposes. Proponents should further note that the MRC, regardless of current volume tier, will increase for Years 2 to 3, and the optional terms (Years 4 and 5), if applicable, annually by the Government of Canada consumer price index rate that is current at that time.

Volume Tier	**Proposed MRC Price**
281 to 300 assets	
301 to 350 assets	
351 to 400 assets	
401 to 450 assets	
451 to 500 assets	
501 or more assets	
TOTAL EXPANSION OF SERVICES MRC	**$**

Note: Proponents should note that as EDC is responsible for Azure Sentinel consumption fees, the provider should be flexible to reduce the number of monitored assets with no penalties. As EDC adds or removes assets, the cost per asset and the new MRC must be determined based on the current quantity and applicable volume tier price. Proponents should note that asset count and integration of new assets will be reconciled on a monthly basis. The following billing month after assets were either added or removed, the new monthly MRC shall be adjusted to reflect the current asset count based on the relevant quantity bracket.

COMMITTED PRICING FOR REQUIREMENTS: (sum of the following: **1. Proposed Initial NRC Price +** **2. Proposed Annual MRC (280 Assets) +** **3. Total Expansion NRC Price +** **4. Total Expansion of Services MRC)**	**$**

The Committed Pricing for Requirements will be scored based on a relative pricing formula using the Committed Pricing for Requirements as the proponent's price. Each proponent will receive a percentage of the total possible points allocated to the Committed Pricing for Requirements, which will be calculated in accordance with the following formula:

$$lowest\ price \div proponent's\ price\ \times\ weighting = proponent's\ pricing\ points$$

ii. Hourly Rates for Resources (5 points)

Provide the hourly rate for each of the roles listed in the table below and as defined in the Deliverables (Section A. of Appendix B). The Total Hourly Rate will be calculated by adding all of the proposed hourly rates and will only be used for scoring purposes. Proponents should note that the proposed hourly rates will increase for Years 2 to 3, and the optional terms (Years 4 and 5), if applicable, annually by the Government of Canada consumer price index rate that is current at that time.

Role	**Proposed Hourly Rate**
Senior Cybersecurity Advisor	
Senior Advisor	
SOC Manager	
Account Executive	
Sentinel SOC Shift Lead	
TOTAL HOURLY RATE (sum of all proposed hourly rate)	**$**

The Hourly Rates for Resources will be scored based on a relative pricing formula using the Total Hourly Rate as the proponent's price. Each proponent will receive a percentage of the total possible points allocated to the Hourly Rates for Resources, which will be calculated in accordance with the following formula:

$$lowest\ price \div proponent's\ price\ \times\ weighting = proponent's\ pricing\ points$$

APPENDIX C – SUBMISSION FORM

1. Proponent Information

Please fill out the following form, naming one (1) person to be the proponent's contact for the RFP process and for any clarifications or communication that might be necessary.	
Full Legal Name of Proponent:	
Any Other Relevant Name under which Proponent Carries on Business:	
Street Address:	
City, Province/State:	
Postal Code:	
Phone Number:	
Company Website (if any):	
Proponent Contact Name and Title:	
Proponent Contact Phone:	
Proponent Contact Email:	

2. Acknowledgment of Non-Binding Procurement Process

The proponent acknowledges that the RFP process will be governed by the terms and conditions of the RFP, and that, among other things, such terms and conditions confirm that this procurement process does not constitute a formal, legally binding bidding process (and for greater certainty, does not give rise to a Contract A bidding process contract), and that no legal relationship or obligation regarding the procurement of any good or service will be created between EDC and the proponent unless and until EDC and the proponent execute a written agreement for the Deliverables.

3. Ability to Provide Deliverables

The proponent has carefully examined the RFP documents and has a clear and comprehensive knowledge of the Deliverables required. The proponent represents and warrants its ability to provide the Deliverables in accordance with the requirements of the RFP for the rates set out in its proposal.

4. Non-Binding Pricing

The proponent has submitted its pricing in accordance with the instructions in the RFP. The proponent confirms that the pricing information provided is accurate. The proponent acknowledges that any inaccurate, misleading, or incomplete information, including withdrawn or altered pricing, could adversely impact the acceptance of its proposal or its eligibility for future work.

5. Addenda

The proponent is deemed to have read and taken into account all addenda issued by EDC prior to the Deadline for Issuing Addenda.

6. Communication with Competitors

For the purposes of this RFP, the word "competitor" includes any individual or organization, other than the proponent, whether or not related to or affiliated with the proponent, who could potentially submit a response to this RFP.

Unless specifically disclosed below under Disclosure of Communications with Competitors, the proponent declares that:

(a) it has prepared its proposal independently from, and without consultation, communication, agreement, or arrangement with any competitor, including, but not limited to, consultation, communication, agreement, or arrangement regarding:

(i) prices;

(ii) methods, factors, or formulas used to calculate prices;

(iii) the quality, quantity, specifications, or delivery particulars of the Deliverables;

(iv) the intention or decision to submit, or not to submit, a proposal; or

(v) the submission of a proposal which does not meet the mandatory technical requirements or specifications of the RFP; and

(b) it has not disclosed details of its proposal to any competitor and it will not disclose details of its proposal to any competitor prior to the notification of the outcome of the procurement process.

Disclosure of Communications with Competitors

If the proponent has communicated or intends to communicate with one (1) or more competitors about this RFP or its proposal, the proponent discloses below the names of those competitors and the nature of, and reasons for, such communications:

_____

_____

_____

_____

_____

_____

7. No Prohibited Conduct

The proponent declares that it has not engaged in any conduct prohibited by this RFP.

8. Conflict of Interest

The proponent must declare all potential Conflicts of Interest, as defined in Section 3.4.1 of the RFP. This includes disclosing the names and all pertinent details of all individuals (employees, advisers, or individuals acting in any other capacity) who (a) participated in the preparation of the proposal; **AND** (b) were employees of EDC within twelve (12) months prior to the Submission Deadline.

If the box below is left blank, the proponent will be deemed to declare that (a) there was no Conflict of Interest in preparing its proposal; and (b) there is no foreseeable Conflict of Interest in performing the contractual obligations contemplated in the RFP.

Otherwise, if the statement below applies, check the box.

3) The proponent declares that there is an actual or potential Conflict of Interest relating to the preparation of its proposal, and/or the proponent foresees an actual or potential Conflict of Interest in performing the contractual obligations contemplated in the RFP.

If the proponent declares an actual or potential Conflict of Interest by marking the box above, the proponent must set out below details of the actual or potential Conflict of Interest:

9. Disclosure of Information

The proponent hereby agrees that any information provided in this proposal, even if it is identified as being supplied in confidence, may be disclosed where required by law or by order of a court or tribunal. The proponent hereby consents to the disclosure, on a confidential basis, of this proposal by EDC to the advisers retained by EDC to advise or assist with the RFP process, including with respect to the evaluation of this proposal.

Signature of Proponent Representative

Name of Proponent Representative

Title of Proponent Representative

Date

I have the authority to bind the proponent.