THE CITY OF WINNIPEG

REQUEST FOR PROPOSAL

RFP NO. 877-2019

SECURITY INFORMATION AND EVENT MANAGEMENT SYSTEM (SIEM)

TABLE OF CONTENTS

PART B - BIDDING PROCEDURES

B1. CONTRACT TITLE

B1.1 SECURITY INFORMATION AND EVENT MANAGEMENT SYSTEM (SIEM)

B2. SUBMISSION DEADLINE

B2.1 The Submission Deadline is 12:00 noon Winnipeg time, October 31, 2019.

B2.2 Proposals determined by the Manager of Materials to have been received later than the Submission Deadline will not be accepted and will be returned upon request.

B2.3 The Contract Administrator or the Manager of Materials may extend the Submission Deadline by issuing an addendum at any time prior to the time and date specified in B2.1.

B3. PROPONENTS' CONFERENCE

B3.1 The Contract Administrator will hold a Proponents' conference at 2:00pm on October 10, 2019 at:

Materials Management

185 King Street

Winnipeg Manitoba

R3B 1J1

B3.2 Bidders unable to physically attend the conference location can contact the Contract Administrator for teleconference contact options.

B3.3 The Proponent shall not be entitled to rely on any information or interpretation received at the Proponents' conference unless that information or interpretation is provided by the Contract Administrator in writing.

B4. ENQUIRIES

B4.1 All enquiries shall be directed to the Contract Administrator identified in D6.1.

B4.2 If the Proponent finds errors, discrepancies or omissions in the Request for Proposal, or is unsure of the meaning or intent of any provision therein, the Proponent shall promptly notify the Contract Administrator of the error, discrepancy or omission at least five (5) Business Days prior to the Submission Deadline.

B4.3 Responses to enquiries which, in the sole judgment of the Contract Administrator, require a correction to or a clarification of the Request for Proposal will be provided by the Contract Administrator to all Proponents by issuing an addendum.

B4.4 Responses to enquiries which, in the sole judgment of the Contract Administrator, do not require a correction to or a clarification of the Request for Proposal will be provided by the Contract Administrator only to the Proponent who made the enquiry.

B4.5 All correspondence or contact by Proponents with the City in respect of this RFP must be directly and only with the Contract Administrator. Failure to restrict correspondence and contact to the Contract Administrator may result in the rejection of the Proponents Proposal Submission.

B4.6 The Proponent shall not be entitled to rely on any response or interpretation received pursuant to B4 unless that response or interpretation is provided by the Contract Administrator in writing.

B5. CONFIDENTIALITY

B5.1 Information provided to a Proponent by the City or acquired by a Proponent by way of further enquiries or through investigation is confidential. Such information shall not be used or disclosed in any way without the prior written authorization of the Contract Administrator. The use and disclosure of the confidential information shall not apply to information which:

(a) was known to the Proponent before receipt hereof; or

(b) becomes publicly known other than through the Proponent; or

(c) is disclosed pursuant to the requirements of a governmental authority or judicial order.

B5.2 The Proponent shall not make any statement of fact or opinion regarding any aspect of the Request for Proposal to the media or any member of the public without the prior written authorization of the Contract Administrator.

B6. ADDENDA

B6.1 The Contract Administrator may, at any time prior to the Submission Deadline, issue addenda correcting errors, discrepancies or omissions in the Request for Proposal, or clarifying the meaning or intent of any provision therein.

B6.2 The Contract Administrator will issue each addendum at least two (2) Business Days prior to the Submission Deadline, or provide at least two (2) Business Days by extending the Submission Deadline.

B6.3 Addenda will be available on the Bid Opportunities page at The City of Winnipeg, Corporate Finance, Materials Management Division website at http://www.winnipeg.ca/matmgt/bidopp.asp

B6.4 The Proponent is responsible for ensuring that he/she has received all addenda and is advised to check the Materials Management Division website for addenda regularly and shortly before the Submission Deadline, as may be amended by addendum.

B6.5 The Proponent shall acknowledge receipt of each addendum in Paragraph 9 of Form A: Proposal. Failure to acknowledge receipt of an addendum may render a Proposal non-responsive.

B6.6 Notwithstanding B4, enquiries related to an Addendum may be directed to the Contract Administrator indicated in D6.

B7. SUBSTITUTES

B7.1 The Work is based on the Plant, Materials and methods specified in the Request for Proposal.

B7.2 Substitutions shall not be allowed unless application has been made to and prior approval has been granted by the Contract Administrator in writing.

B7.3 Requests for approval of a substitute will not be considered unless received in writing by the Contract Administrator at least five (5) Business Days prior to the Submission Deadline.

B7.4 The Proponent shall ensure that any and all requests for approval of a substitute:

(a) provide sufficient information and details to enable the Contract Administrator to determine the acceptability of the Plant, Material or method as either an approved equal or alternative;

(b) identify any and all changes required in the applicable Work, and all changes to any other Work, which would become necessary to accommodate the substitute;

(c) identify any anticipated cost or time savings that may be associated with the substitute;

(d) certify that, in the case of a request for approval as an approved equal, the substitute will fully perform the functions called for by the general design, be of equal or superior

substance to that specified, is suited to the same use and capable of performing the same function as that specified and can be incorporated into the Work, strictly in accordance with the Contract;

(e) certify that, in the case of a request for approval as an approved alternative, the substitute will adequately perform the functions called for by the general design, be similar in substance to that specified, is suited to the same use and capable of performing the same function as that specified and can be incorporated into the Work, strictly in accordance with the Contract.

B7.5 The Contract Administrator, after assessing the request for approval of a substitute, may in his/her sole discretion grant approval for the use of a substitute as an "approved equal" or as an "approved alternative", or may refuse to grant approval of the substitute.

B7.6 The Contract Administrator will provide a response in writing, at least two (2) Business Days prior to the Submission Deadline, to the Proponent who requested approval of the substitute.

B7.6.1 The Contract Administrator will issue an Addendum, disclosing the approved materials, equipment, methods and products to all potential Proponents. The Proponent requesting and obtaining the approval of a substitute shall be responsible for disseminating information regarding the approval to any person or persons he/she wishes to inform.

B7.7 If the Contract Administrator approves a substitute as an "approved equal", any Proponent may use the approved equal in place of the specified item.

B7.8 If the Contract Administrator approves a substitute as an "approved alternative", any Proponent bidding that approved alternative may base his/her Total Bid Price upon the specified item but may also indicate an alternative price based upon the approved alternative. Such alternatives will be evaluated in accordance with B23.

B7.9 No later claim by the Contractor for an addition to the Total Bid Price because of any other changes in the Work necessitated by the use of an approved equal or an approved alternative will be considered.

B8. PROPOSAL SUBMISSION

B8.1 The Proposal shall consist of the following components:

(a) Form A: Proposal; and

(b) Form B: Prices.

B8.2 The Proposal should also consist of the following components:

(a) Experience of Proponent and Subcontractors (Section C) in accordance with B11;

(b) Experience of Key Personnel Assigned to the Project (Section D), in accordance with B12;

(c) Project Understanding and Methodology (Section E) in accordance with B13; and

(d) Technical Requirements (Section F) in accordance with B14.

B8.3 Further to B8.1 all components of the Proposal shall be fully completed or provided in the order indicated, and submitted by the Proponent no later than the Submission Deadline, with all required entries made clearly and completely, to constitute a responsive Proposal.

B8.4 Further to B8.2, all components of the Proposal should be fully completed or provided in the order indicated, and submitted by the Proponent no later than the Submission Deadline, with all required entries made clearly and completely.

B8.5 Proponents should submit one (1) unbound 8.5" x 11" original (marked "original") including drawings and three (3) copies (copies can be in any size format) for sections identified in B8.1and B8.2.

B8.6 Proposal format, including type of binding, number of pages, size of pages and, font, etc., will not be regulated, except that the Proposal should contain a table of contents, page numbering and should be in the Sections identified above. Proponents are encouraged to use their creativity to submit a Proposal which provides the requested information for evaluation and other information which illustrates the strength of their team.

B8.7 Proponents are advised that inclusion of terms and conditions inconsistent with the Request for Proposal, will be evaluated in accordance with B23.1(a).

B8.8 The Proposal shall be submitted enclosed and sealed in an envelope/package clearly marked with the RFP number and the Proponent's name and address.

B8.9 Proposals submitted by facsimile transmission (fax) or internet electronic mail (e-mail) will not be accepted.

B8.10 Proposals shall be submitted to:

The City of Winnipeg
Corporate Finance Department
Materials Management Division
185 King Street, Main Floor
Winnipeg MB R3B 1J1

B8.11 Any cost or expense incurred by the Proponent that is associated with the preparation of the Proposal shall be borne solely by the Proponent.

B9. PROPOSAL

B9.1 The Proponent shall complete Form A: Proposal, making all required entries.

B9.2 Paragraph 2 of Form A: Proposal shall be completed in accordance with the following requirements:

(a) if the Proponent is a sole proprietor carrying on business in his/her own name, his/her name shall be inserted;

(b) if the Proponent is a partnership, the full name of the partnership shall be inserted;

(c) if the Proponent is a corporation, the full name of the corporation shall be inserted;

(d) if the Proponent is carrying on business under a name other than his/her own, the business name and the name of every partner or corporation who is the owner of such business name shall be inserted.

B9.2.1 If a Proposal is submitted jointly by two or more persons, each and all such persons shall identify themselves in accordance with B9.2.

B9.3 In Paragraph 3 of Form A: Proposal, the Proponent shall identify a contact person who is authorized to represent the Proponent for purposes of the Proposal.

B9.4 Paragraph 0 of Form A: Proposal shall be signed in accordance with the following requirements:

(a) if the Proponent is a sole proprietor carrying on business in his/her own name, it shall be signed by the Proponent;

(b) if the Proponent is a partnership, it shall be signed by the partner or partners who have authority to sign for the partnership;

(c) if the Proponent is a corporation, it shall be signed by its duly authorized officer or officers and the corporate seal, if the corporation has one, should be affixed;

(d) if the Proponent is carrying on business under a name other than his/her own, it shall be signed by the registered owner of the business name, or by the registered owner's authorized officials if the owner is a partnership or a corporation.

B9.4.1 The name and official capacity of all individuals signing Form A: Proposal should be printed below such signatures.

B9.5 If a Proposal is submitted jointly by two or more persons, the word "Proponent" shall mean each and all such persons, and the undertakings, covenants and obligations of such joint Proponents in the Proposal and the Contract, when awarded, shall be both joint and several.

B10. PRICES

B10.1 The Proponent shall state a price in Canadian funds for each item of the Work identified on Form B: Prices. The lump sum Price shall include a detailed itemised cost breakdown of all the included items of the proposed solution. For example:

(a) Final purchase, deployment, 1st year subscription and support cost
  (i) include detailed breakdown of items (including hardware and software)
  (ii) Services for installation assistance (including ingestion of all data sources)

(b) Total cost of professional services
  (i) Design & specification/requirements gathering and documentation
  (ii) SIEM tuning and system customization
  (iii) Testing and Go-Live
  (iv) Project Management
  (v) Travel Costs & Living Expenses

(c) Total cost of software
  (i) Licensing/Subscription (including any third party software licenses)

(d) Cost of training for approximately 5 Administrators (configuration & administration).

B10.1.1 Notwithstanding C11.1.3, prices on Form B: Prices shall not include the Goods and Services Tax (GST) or Manitoba Retail Sales Tax (MRST, also known as PST), which shall be extra where applicable.

B10.2 The quantities listed on Form B: Prices are to be considered approximate only. The City will use said quantities for the purpose of comparing Proposals.

B10.3 The quantities for which payment will be made to the Contractor are to be determined by the Work actually performed and completed by the Contractor, to be measured as specified in the applicable Specifications.

B10.4 Payments to Non-Resident Contractors are subject to Non-Resident Withholding Tax pursuant to the Income Tax Act (Canada).

B11. EXPERIENCE OF PROPONENT AND SUBCONTRACTORS (SECTION C)

B11.1 Proposals should include:

(a) details demonstrating the history and experience of the Proponent and Subcontractors in providing programming; design, management of implementation and contract administration services on up to three projects of similar complexity, scope and value.

B11.2 For each project listed in B11.1(a), the Proponent should submit:

(a) description of the project;

(b) role of the contractor;

(c) percentage variation in project's original contracted cost and final cost;

(d) design and implementation schedule (anticipated Project schedule and actual project delivery schedule, showing design and implementation separately);

(e) project owner;

(f) reference information (one current name with telephone number per project).

B11.2.1 Where applicable, information should be separated into Proponent and Subcontractor project listings.

B11.3 The Proposal should include general firm profile information, including

(a) years in business;

(b) average volume of work; and

(c) number of employees.

B12. EXPERIENCE OF KEY PERSONNEL ASSIGNED TO THE PROJECT (SECTION D)

B12.1 Describe your approach to overall team formation and coordination of team members.

B12.1.1 Include an organizational chart for the Project.

B12.2 Submit the experience and qualifications of the Key Personnel assigned to the Project for projects of similar complexity, scope and value, including the principals-in-charge, the Contractors Representative, managers of the key disciplines and lead designers. Include educational background and degrees, professional recognition, job title, years of experience in current position, years of experience in design and implementation, and years of experience with existing employer. Roles of each of the Key Personnel in the Project should be identified in the organizational chart referred to in B12.1.1.

B12.3 For each person identified, list at least two comparable projects in which they have played a primary role. If a project selected for a key person is included in B11, provide only the project name and the role of the key person. For other projects provide the following:

(a) Description of project;

(b) Role of the person;

(c) Project Owner;

(d) Reference information (one current name with telephone number per project).

B13. PROJECT UNDERSTANDING AND METHODOLOGY (SECTION E)

B13.1 Describe your firm's project management approach and team organization during the performance of Services, so that the evaluation committee has a clear understanding of the methods the Proponent will use in the delivery of this Project.

B13.2 Methodology should be presented in accordance with the Scope of Services identified in D3. Describe the collaborative process/method to be used by the Key Personnel of the team in the various phases of the Project.

B13.3 Proposals should address:

(a) the team's understanding of the broad functional and technical requirements;

(b) the proposed Project budget;

(c) the City's Project methodology with respect to the information provided within this RFP and the City's Project Management Manual at http://winnipeg.ca/infrastructure/asset-management-program/templates-manuals.stm#2 and templates at http://winnipeg.ca/infrastructure/asset-management-program/templates-manuals.stm#4 ; and;

(d) any other issue that conveys your team's understanding of the Project requirements.

B13.4 For each person identified in B12.2, list the percent of time to be dedicated to the Project in accordance with the Scope of Services identified in D3.

B14. TECHNICAL REQUIREMENTS (SECTION F)

B14.1 Describe the architecture of the proposed SIEM solution. Provide diagrams detailing the solution.

B14.2 Provide details on how the SIEM solution would collect logs and flows from the City of Winnipeg environment.

B14.3 Itemize and describe all of the SIEM hardware, software, and service components of the proposed solution. Ensure to identify the device's manufacturer and model as well as the performance and capacity capability of the recommended device(s).

B14.4 Describe how the SIEM solution is capable of ensuring that no log data is lost due to any failure of any component of the system.

B14.5 Describe how the event log information will be collected using agent-based or agentless collectors.

B14.6 Describe how (i.e. method, time-lines, costs, etc.) a new piece of equipment, or a new technology, acquired by City of Winnipeg would be integrated to be monitored by the SIEM.

B14.7 Describe how the SIEM solution provides for and integrates into the following use cases:

(a) Incident Response;

(b) Threat Hunting;

(c) Malware Tracking.

B14.8 Describe the process (i.e. methods, time-lines, costs, etc.) of adding additional use-case scenarios.

B14.9 Describe what threat intelligence feeds are included with your solution and how they are integrated to the required use cases.

B14.10 Identify the bandwidth required if solution collectors send information to other solution devices.

B14.11 Describe what data compression technologies are utilized or supported by the solution.

B14.12 Describe how the SIEM solution reports on the health of all hardware and software required to operate the system.

B14.13 Describe the SIEM solution's reporting capabilities including both manual and automated reports as well as their customization options. Provide examples of predefined and customized reports.

B14.14 Describe the SIEM solution's dashboard and how it can be customized. Provide examples of predefined and custom dashboard reports/screens.

B14.15 Describe the SIEM solution's alerting system, specifically how the alerts display severity of alert and the supporting information contained in the alert for investigation. Describe methods for integrating the alerting system with other City of Winnipeg systems.

B14.16 Describe how the solution scales to increased demand placed on the solution as the organization adds more devices, locations, applications, etc. Describe the impact to each of the proposed components of the solution (i.e. appliances, storage, management consoles, etc.).

B15. DISCLOSURE

B15.1 Various Persons provided information or services with respect to this Work. In the City's opinion, this relationship or association does not create a conflict of interest because of this full

disclosure. Where applicable, additional material available as a result of contact with these Persons is listed below.

B15.2 The Persons are:

(a) McAfee;

(b) Scalar;

(c) Splunk;

(d) Telus;

(e) LogRhythm;

(f) RSA;

(g) Horizon;

(h) IBM.

B16. CONFLICT OF INTEREST AND GOOD FAITH

B16.1 Proponents, by responding to this RFP, declare that no Conflict of Interest currently exists, or is reasonably expected to exist in the future.

B16.2 Conflict of Interest means any situation or circumstance where a Proponent or Key Personnel proposed for the Work has:

(a) other commitments;

(b) relationships;

(c) financial interests; or

(d) involvement in ongoing litigation;

that could or would be seen to:

(i) exercise an improper influence over the objective, unbiased and impartial exercise of the independent judgment of the City with respect to the evaluation of Proposals or award of the Contract; or

(ii) compromise, impair or be incompatible with the effective performance of a Proponent's obligations under the Contract;

(e) has contractual or other obligations to the City that could or would be seen to have been compromised or impaired as a result of its participation in the RFP process or the Project; or

(f) has knowledge of confidential information (other than confidential information disclosed by the City in the normal course of the RFP process) of strategic and/or material relevance to the RFP process or to the Project that is not available to other proponents and that could or would be seen to give that Proponent an unfair competitive advantage.

B16.3 In connection with its Proposal, each entity identified in B16.2 shall:

(a) avoid any perceived, potential or actual Conflict of Interest in relation to the procurement process and the Project;

(b) upon discovering any perceived, potential or actual Conflict of Interest at any time during the RFP process, promptly disclose a detailed description of the Conflict of Interest to the City in a written statement to the Project Manager; and

(c) provide the City with the proposed means to avoid or mitigate, to the greatest extent practicable, any perceived, potential or actual Conflict of Interest and shall submit any additional information to the City that the City considers necessary to properly assess the perceived, potential or actual Conflict of Interest.

B16.4 Without limiting B16.3, the City may, in its sole discretion, waive any and all perceived, potential or actual Conflicts of Interest. The City's waiver may be based upon such terms and conditions

as the City, in its sole discretion, requires to satisfy itself that the Conflict of Interest has been appropriately avoided or mitigated, including requiring the Proponent to put into place such policies, procedures, measures and other safeguards as may be required by and be acceptable to the City, in its sole discretion, to avoid or mitigate the impact of such Conflict of Interest.

B16.5 Without limiting B16.3, and in addition to all contractual or other rights or rights at law or in equity or legislation that may be available to the City, the City may, in its sole discretion:

(a) disqualify a Proponent that fails to disclose a perceived, potential or actual Conflict of Interest of the Proponent or any of its Key Personnel;

(b) require the removal or replacement of any Key Personnel proposed for the Work that has a perceived, actual or potential Conflict of Interest that the City, in its sole discretion, determines cannot be avoided or mitigated;

(c) disqualify a Proponent or Key Personnel proposed for the Work that fails to comply with any requirements prescribed by the City pursuant to B16.4 to avoid or mitigate a Conflict of Interest; and

(d) disqualify a Proponent if the Proponent, or one of its Key Personnel proposed for the Project, has a perceived, potential or actual Conflict of Interest that, in the City's sole discretion, cannot be avoided or mitigated, or otherwise resolved.

B16.6 The final determination of whether a perceived, potential or actual Conflict of Interest exists shall be made by the City, in its sole discretion.

B17. QUALIFICATION

B17.1 The Proponent shall:

(a) undertake to be in good standing under The Corporations Act (Manitoba), or properly registered under The Business Names Registration Act (Manitoba), or otherwise properly registered, licensed or permitted by law to carry on business in Manitoba, or if the Proponent does not carry on business in Manitoba, in the jurisdiction where the Proponent does carry on business; and

(b) be financially capable of carrying out the terms of the Contract; and

(c) have all the necessary experience, capital, organization, and equipment to perform the Work in strict accordance with the terms and provisions of the Contract.

B17.2 The Proponent and any proposed Subcontractor (for the portion of the Work proposed to be subcontracted to them) shall:

(a) be responsible and not be suspended, debarred or in default of any obligations to the City. A list of suspended or debarred individuals and companies is available on the Information Connection page at The City of Winnipeg, Corporate Finance, Materials Management Division website at https://winnipeg.ca/finance/findata/matmgt/listing/debar.pdf

B17.3 The Proponent and/or any proposed Subcontractor (for the portion of the Work proposed to be subcontracted to them) shall:

(a) have successfully carried out work similar in nature, scope and value to the Work; and

(b) be fully capable of performing the Work required to be in strict accordance with the terms and provisions of the Contract; and

B17.4 The Proponent shall submit, within three (3) Business Days of a request by the Contract Administrator, proof satisfactory to the Contract Administrator of the qualifications of the Proponent and of any proposed Subcontractor.

B18. OPENING OF PROPOSALS AND RELEASE OF INFORMATION

B18.1 Proposals will not be opened publicly.

B18.2 After award of Contract, the names of the Proponents and the Contract amount of the successful Proponent and their address(es) will be available on the Closed Bid Opportunities (or Public/Posted Opening & Award Results) page at The City of Winnipeg, Corporate Finance, Materials Management Division website at http://www.winnipeg.ca/matmgt/

B18.3 The Proponent is advised that any information contained in any Proposal Submission may be released if required by The Freedom of Information and Protection of Privacy Act (Manitoba), by other authorities having jurisdiction, or by law or by City policy or procedures (which may include access by members of City Council).

B18.3.1 To the extent permitted, the City shall treat as confidential information, those aspects of a Proposal Submission identified by the Proponent as such in accordance with and by reference to Part 2, Section 17 or Section 18 or Section 26 of The Freedom of Information and Protection of Privacy Act (Manitoba), as amended.

B18.4 Following the award of Contract, a Proponent will be provided with information related to the evaluation of his/her submission upon written request to the Contract Administrator.

B19. IRREVOCABLE OFFER

B19.1 The Proposal(s) submitted by the Proponent shall be irrevocable for the time period specified in Paragraph 10 of Form A: Proposal.

B19.2 The acceptance by the City of any Proposal shall not release the Proposals of the other responsive Proponents and these Proponents shall be bound by their offers on such Work for the time period specified in Paragraph 10 of Form A: Proposal.

B20. WITHDRAWAL OF OFFERS

B20.1 A Proponent may withdraw his/her Proposal without penalty by giving written notice to the Manager of Materials at any time prior to the Submission Deadline.

B20.1.1 Notwithstanding C22.5, the time and date of receipt of any notice withdrawing a Proposal shall be the time and date of receipt as determined by the Manager of Materials.

B20.1.2 The City will assume that any one of the contact persons named in Paragraph 3 of Form A: Proposal or the Proponent's authorized representatives named in Paragraph 0 of Form A: Proposal, and only such person, has authority to give notice of withdrawal.

B20.1.3 If a Proponent gives notice of withdrawal prior to the Submission Deadline, the Manager of Materials will:

(a) retain the Proposal until after the Submission Deadline has elapsed;

(b) open the Proposal to identify the contact person named in Paragraph 3 of Form A: Proposal and the Proponent's authorized representatives named in Paragraph 0 of Form A: Proposal; and

(c) if the notice has been given by any one of the persons specified in B20.1.3(b), declare the Proposal withdrawn.

B20.2 A Proponent who withdraws his/her Proposal after the Submission Deadline but before his/her offer has been released or has lapsed as provided for in B19.2 shall be liable for such damages as are imposed upon the Proponent by law and subject to such sanctions as the Chief Administrative Officer considers appropriate in the circumstances. The City, in such event, shall be entitled to all rights and remedies available to it at law.

B21. INTERVIEWS

B21.1 The Contract Administrator may, in his/her sole discretion, interview Proponents during the evaluation process.

B21.2 The Contract Administrator may, in his/her sole discretion, ask Proponents to provide product demonstrations to given scenarios.

B22. NEGOTIATIONS

B22.1 The City reserves the right to negotiate details of the Contract with any Proponent. Proponents are advised to present their best offer, not a starting point for negotiations in their Proposal Submission.

B22.2 The City may negotiate with the Proponents submitting, in the City's opinion, the most advantageous Proposals. The City may enter into negotiations with one or more Proponents without being obligated to offer the same opportunity to any other Proponents. Negotiations may be concurrent and will involve each Proponent individually. The City shall incur no liability to any Proponent as a result of such negotiations.

B22.3 If, in the course of negotiations pursuant to B22.2, the Proponent amends or modifies a Proposal after the Submission Deadline, the City may consider the amended Proposal as an alternative to the Proposal already submitted without releasing the Proponent from the Proposal as originally submitted.

B23. EVALUATION OF PROPOSALS

B23.1 Award of the Contract shall be based on the following evaluation criteria:

(a)	compliance by the Proponent with the requirements of the Request for Proposal or acceptable deviation therefrom:	(pass/fail)
(b)	qualifications of the Proponent and the Subcontractors, if any, pursuant to B17:	(pass/fail)
(c)	Total Bid Price;	40%
(d)	Experience of Proponent and Subcontractor; (Section C)	15%
(e)	Experience of Key Personnel Assigned to the Project; (Section D)	5%
(f)	Project Understanding and Methodology (Section E)	5%
(g)	Technical Requirements. (Section F)	35%

B23.2 Further to B23.1(a), the Award Authority may reject a Proposal as being non-responsive if the Proposal is incomplete, obscure or conditional, or contains additions, deletions, alterations or other irregularities. The Award Authority may reject all or any part of any Proposal, or waive technical requirements or minor informalities or irregularities if the interests of the City so require.

B23.3 Further to B23.1(b) the Award Authority shall reject any Proposal submitted by a Proponent who does not demonstrate, in his/her Proposal or in other information required to be submitted, that he/she is qualified.

B23.4 If, in the sole opinion of the City, a Proposal does not achieve a pass rating for B23.1(a) and B23.1(b), the Proposal will be determined to be non-responsive and will not be further evaluated.

B23.5 Where references are requested, the reference checks to confirm information provided may not be restricted to only those submitted by the Proponent, and may include organizations representing Persons, known to have done business with the Proponent.

B23.6 Further to B23.1(c), the Total Bid Price shall be the lump sum price shown on Form B: Prices.

B23.7 Further to B23.1(d), Experience of Proponent and Subcontractors will be evaluated considering the experience of the organization on projects of similar size and complexity as well as other information requested, in accordance with B11.

B23.8 Further to B23.1(e), Experience of Key Personnel Assigned to the Project will be evaluated considering the experience and qualifications of the Key Personnel and Subcontractor personnel on Projects of comparable size and complexity, in accordance with B12.

B23.9 Further to B23.1(f), Project Understanding and Methodology will be evaluated considering your firm's understanding of the City's Project, project management approach and team organization, in accordance with B13.

B23.10 Further to B23.1(g), Technical Requirements will be evaluated considering the Proponent's ability to comply with the requirements of the Project, in accordance with B14.

B23.11 Notwithstanding B23.1(d) to B23.1(g), where Proponents fail to provide a response to B8.2(a) to B8.2(d), the score of zero may be assigned to the incomplete part of the response.

B23.12 This Contract will be awarded as a whole.

B23.13 Proposals will be evaluated considering the information in the Proposal Submission and any interviews held in accordance with B21.

B24. AWARD OF CONTRACT

B24.1 The City will give notice of the award of the Contract, or will give notice that no award will be made.

B24.2 The City will have no obligation to award a Contract to a Proponent, even though one or all of the Proponents are determined to be qualified, and the Proposals are determined to be responsive.

B24.2.1 Without limiting the generality of B24.2, the City will have no obligation to award a Contract where:

(a) the prices exceed the available City funds for the Work;

(b) the prices are materially in excess of the prices received for similar work in the past;

(c) the prices are materially in excess of the City's cost to perform the Work, or a significant portion thereof, with its own forces;

(d) only one Proposal is received; or

(e) in the judgment of the Award Authority, the interests of the City would best be served by not awarding a Contract.

B24.3 Where an award of Contract is made by the City, the award shall be made to the qualified Proponent submitting the most advantageous offer.

B24.3.1 Following the award of contract, a Proponent will be provided with information related to the evaluation of his/her Proposal upon written request to the Contract Administrator.

B24.4 Notwithstanding C4, the City may issue a purchase order to the successful Proponent in lieu of the execution of a Contract.

B24.5 The Contract Documents, as defined in C1.1(n)(ii), in their entirety shall be deemed to be incorporated in and to form a part of the purchase order notwithstanding that they are not necessarily attached to or accompany said purchase order.

PART C - GENERAL CONDITIONS

C0. GENERAL CONDITIONS

C0.1 The *General Conditions for Supply of Services* (Revision 2019-01-15) are applicable to the Work of the Contract.

C0.1.1 The *General Conditions for Supply of Services* are available on the Information Connection page at The City of Winnipeg, Corporate Finance, Materials Management Division website at http://www.winnipeg.ca/matmgt/gen_cond.stm

C0.1.2 A reference in the Request for Proposal to a section, clause or subclause with the prefix "**C**" designates a section, clause or subclause in the *General Conditions for Supply of Services*

PART D - SUPPLEMENTAL CONDITIONS

GENERAL

D1. GENERAL CONDITIONS

D1.1 In addition to the *General Conditions for Supply of Services*, these Supplemental Conditions are applicable to the Work of the Contract.

D2. BACKGROUND

D2.1 The City of Winnipeg currently has two active data centers, which host virtualized and physical systems. These data centers are connected via multiple 10Gb/s connections.

D2.2 The City of Winnipeg currently has approximately 200 remote sites connected to the core data centers via VPLS networks aggregated over six 1 Gb/s head-end connections.

D2.3 The City of Winnipeg currently has a small footprint in the Microsoft Azure IaaS environment, connected to the aforementioned datacenters via a 100mbps VPN link.

D2.4 The City of Winnipeg utilizes the following technologies that may be relevant to a SIEM implementation:

(a) Check Point Firewalls
    (i) Utilizing all software blades
(b) Cisco Routers and Switches
(c) Cisco Wireless LAN Controllers
(d) F5 Application Delivery Controllers
    (i) APM, ASM and LTM blades
(e) InfoBlox DHCP and DNS appliances
(f) Windows 2012 Domain Controllers
(g) Windows 2012, 2016 and 2019 Servers
(h) Windows 10 workstations
(i) Ubuntu 18.04 servers
(j) Symantec Endpoint Protection
    (i) Utilizing on premise management console
(k) Symantec Messaging Gateway (on premise)

D2.5 The measured events per second for the above technologies is 3,000 eps peak and 1,800 eps on a 24-hour average

D3. SCOPE OF SERVICES

D3.1 The Work to be done under the Contract shall include the supply, delivery, installation and configuration of a on premise SIEM solution and maintenance, support and upgrades for three years from the date of execution with the option of three (3) mutually agreed upon one (1) year extensions for License, maintenance, support and upgrades.

D3.1.1 The City may negotiate the extension option with the Contractor within ninety (90) Calendar Days prior to the expiry date of the Contract. The City shall incur no liability to the Contractor as a result of such negotiations.

D3.1.2 Changes resulting from such negotiations shall become effective on anniversary of start date of respective yea. Changes to the Contract shall not be implemented by the Contractor without written approval by the Contract Administrator.

D3.2 The major components of the Work are as follows:

(a) Provision of all software, licenses/subscriptions and hardware required to provide a SIEM solution for the City of Winnipeg based upon the requirements as laid out in.

(b) Services for installation assistance (including ingestion of all data sources listed in D2.4), SIEM tuning and system customization for the following use cases:

(i) Incident Response;

(ii) Malware Tracking and;

(iii) Threat Hunting.

(c) Provision for all required threat feed and software subscriptions as well as support for three (3) years.

D3.3 The funds available for this Contract are $423,000.00 (CAD).

D3.3 Notwithstanding D3.1, the type and quantity of Work to be performed under this Contract is subject to annual approval of monies therefore in a budget by Council. Proponents are advised that monies have been approved for work up to and including December 31, 2019.

D3.3.1 In the event that Council does not approve the annual budget for any year during this Contract, the City reserves the right to alter the type or quantity of work performed under this Contract, or to terminate the Contract, upon one hundred and twenty (120) Calendar Days written notice by the Contract Administrator. In such an event, no claim may be made against the City for damages of any kind resulting from the termination, including, but not limited to, on the ground of loss of anticipated profit on Work.

D3.4 Notwithstanding D3.1, in the event that operational changes result in substantial changes to the requirements for Work, the City reserves the right to alter the type or quantity of work performed under this Contract, or to terminate the Contract, upon thirty (30) Calendar Days written notice by the Contract Administrator. In such an event, no claim may be made for damages on the ground of loss of anticipated profit on Work.

D4. COOPERATIVE PURCHASE

D4.1 The Contractor is advised that this is a cooperative purchase.

D4.2 The Contract Administrator may, from time to time during the term of the Contract, approve other public sector organizations and utilities, including but not limited to municipalities, universities, schools and hospitals, to be participants in the cooperative purchase.

D4.3 The Contract Administrator will notify the Contractor of a potential participant and provide a list of the delivery locations and estimated quantities.

D4.4 If any location of the potential participant is more than ten (10) kilometers beyond the boundaries of the City of Winnipeg, the Contractor shall, within fifteen (15) Calendar Days of the written notice, notify the Contract Administrator of the amount of any additional delivery charge for the location.

D4.5 If any additional delivery charges are identified by the Contractor, the potential participant may accept or decline to participate in the cooperative purchase.

D4.6 The Contractor shall enter into a contract with each participant under the same terms and conditions as this Contract except:

(a) supply under the contract shall not commence until the expiry or lawful termination of any other contract(s) binding the participant for the same services;

(b) a participant may specify a duration of Contract shorter than the duration of this Contract;

(c) a participant may specify that only some items under this Contract and/or less than its total requirement for an item are to be supplied under its contract; and

(d) any additional delivery charge identified and accepted in accordance with clause D4.4 and D4.5 will apply.

D4.7 Each participant will be responsible for the administration of its contract and the fulfilment of its obligations under its contract. The City shall not incur any liability arising from any such contract.

D4.8 No participant shall have the right or authority to effect a change in the Contract, or of any other participant in this Contract.

D5. DEFINITIONS

D5.1 When used in this Request for Proposal:

(a) "**Proponent**" means any Person or Persons submitting a Proposal for Services;

D6. CONTRACT ADMINISTRATOR

D6.1 The Contract Administrator is:

Nick Procyk
Information Security Coordinator

Telephone No. 204 232-9270
Email Address:. nprocyk@winnipeg.ca

D6.2 At the pre-commencement meeting, the Contract Administrator will identify additional personnel representing the Contract Administrator and their respective roles and responsibilities for the Work.

D6.3 Proposal Submissions must be submitted to the address in B8.

D7. OWNERSHIP OF INFORMATION, CONFIDENTIALITY AND NON DISCLOSURE

D7.1 The Contract, all deliverables produced or developed, and information provided to or acquired by the Contractor are the property of the City and shall not be appropriated for the Contractors own use, or for the use of any third party.

D7.2 The Contractor shall not make any public announcements or press releases regarding the Contract, without the prior written authorization of the Contract Administrator.

D7.3 The following shall be confidential and shall not be disclosed by the Contractor to the media or any member of the public without the prior written authorization of the Contract Administrator;

(a) information provided to the Contractor by the City or acquired by the Contractor during the course of the Work;

(b) the Contract, all deliverables produced or developed; and

(c) any statement of fact or opinion regarding any aspect of the Contract.

D7.4 A Contractor who violates any provision of D7 may be determined to be in breach of Contract.

D8. NOTICES

D8.1 Notwithstanding C22.3, all notices of appeal to the Chief Administrative Officer shall be sent to the attention of the Chief Financial Officer.

SUBMISSIONS

D9. AUTHORITY TO CARRY ON BUSINESS

D9.1 The Contractor shall be in good standing under The Corporations Act (Manitoba), or properly registered under The Business Names Registration Act (Manitoba), or otherwise properly registered, licensed or permitted by law to carry on business in Manitoba, or if the Contractor does not carry on business in Manitoba, in the jurisdiction where the Contractor does carry on business, throughout the term of the Contract, and shall provide the Contract Administrator with evidence thereof upon request.

D10. SAFE WORK PLAN

D10.1 The Contractor shall provide the Contract Administrator with a Safe Work Plan at least five (5) Business Days prior to the commencement of any Work on the Site but in no event later than the date specified in C4.1 for the return of the executed Contract.

D10.2 The Safe Work Plan should be prepared and submitted in the format shown in the City's template which is available on the Information Connection page at The City of Winnipeg, Corporate Finance, Materials Management Division website at http://www.winnipeg.ca/matmgt/safety/default.stm

D11. INSURANCE

D11.1 The Contractor shall provide and maintain the following insurance coverage:

(a) commercial general liability insurance, in the amount of at least two million dollars ($2,000,000.00) inclusive, with The City of Winnipeg added as an additional insured; such liability policy to also contain a cross-liability clause, non-owned automobile liability and products and completed operations cover, to remain in place at all times during the performance of the Work;

(b) if applicable, Automobile Liability Insurance covering all motor vehicles, owned and operated and used or to be used by the Contractor directly or indirectly in the performance of the Service. The Limit of Liability shall not be less than $2,000,000 inclusive for loss or damage including personal injuries and death resulting from any one accident or occurrence.

D11.2 Deductibles shall be borne by the Contractor.

D11.3 The Contractor shall provide the Contract Administrator with a certificate(s) of insurance, in a form satisfactory to the City Solicitor, at least two (2) Business Days prior to the commencement of any Work on the Site.

D11.4 The Contractor shall not cancel, materially alter, or cause the policy to lapse without providing at least thirty (30) Calendar Days prior written notice to the Contract Administrator.

D11.5 The City shall have the right to alter the limits and/or coverages as reasonably required from time to time during the continuance of this agreement.

CONTROL OF WORK

D12. COMMENCEMENT

D12.1 The Contractor shall not commence any Work until he/she is in receipt of a notice of award from the City authorizing the commencement of the Work.

D12.2 The Contractor shall not commence any Work on the Site until:

(a) the Contract Administrator has confirmed receipt and approval of:

(i) evidence of authority to carry on business specified in D9;

(ii) evidence of the workers compensation coverage specified in C6.14;

(iii) the Safe Work Plan specified in D10 and;

(iv) evidence of the insurance specified in D11.

(b) the Contractor has attended a meeting with the Contract Administrator, or the Contract Administrator has waived the requirement for a meeting.

D13. ORDERS

D13.1 The Contractor shall provide a local Winnipeg telephone number or a toll-free telephone number at which orders for service may be placed.

D14. RECORDS

D14.1 The Contractor shall keep detailed records of the services supplied under the Contract.

D14.2 The Contractor shall record, as a minimum, for each item listed on Form B: Prices:

(a) user name(s) and addresses;

(b) order date(s);

(c) service date(s); and

(d) description and quantity of services provided.

D14.3 The Contractor shall provide the Contract Administrator with a copy of the records for each quarter year within fifteen (15) Calendar Days of a request of the Contract Administrator.

MEASUREMENT AND PAYMENT

D15. INVOICES

D15.1 Further to C11, the Contractor shall submit an invoice for each portion of Work performed to:

The City of Winnipeg
Corporate Finance - Accounts Payable
4th Floor, Administration Building, 510 Main Street
Winnipeg MB R3B 1B9

Facsimile No.: 204 949-0864
Email: CityWpgAP@winnipeg.ca

D15.2 Invoices must clearly indicate, as a minimum:

(a) the City's purchase order number;

(b) date of delivery;

(c) delivery address;

(d) type and quantity of work performed;

(e) the amount payable with GST and MRST shown as separate amounts; and

(f) the Contractor's GST registration number.

D15.3 The City will bear no responsibility for delays in approval of invoices which are improperly submitted.

D15.4 **Proposal Submissions must not be submitted to the above facsimile number. Proposals must be submitted in accordance with B8**.

D16. PAYMENT

D16.1 Further to C11, payment shall be in Canadian funds net thirty (30) Calendar Days after receipt and approval of the Contractor's invoice.

D16.2 Further to C11, the City may at its option pay the Contractor by direct deposit to the Contractor's banking institution.

WARRANTY

D17. WARRANTY

D17.1 Notwithstanding C12, the warranty period shall be three (3) years from the date of execution of the Work.

PART E - SPECIFICATIONS

GENERAL

E1. APPLICABLE SPECIFICATIONS

E1.1 These Specifications shall apply to the Work.

E1.2 Proponents are reminded that requests for approval of substitutes as an approved equal or an approved alternative shall be made in accordance with B7. In every instance where a brand name or design specification is used, the City will also consider approved equals and/or approved alternatives in accordance with B7.

E2. SIEM SOLUTION REQUIREMENTS

E2.1 The Contractor shall supply, deliver, install and configure a on premise SIEM solution in accordance with the requirements hereinafter specified.

E2.2 Specifications:

#	Requirement
1.	The solution must provide central management of all components and administrative functions from a single web-based user interface.
2.	The administrator must be able to define role base access to the system by device, device group or network range. This includes being able to restrict a user's access to information to only those systems from a specific group of devices or network range.
3.	The administrator must be able to define role-based access to various functional areas of the solution. This includes being able to restrict a user's access to specific functions of the solution that is not within the scope of a user's role including, but not limited to, administration, reporting, event filtering, correlation, and/or dashboard viewing.
4.	The solution must support auto discovery of assets that are being protected or monitored.
5.	The solution must provide an open API for access to data stored within the information database(s).
6.	The solution must provide the ability to encrypt communications between components.
7.	The solution must integrate with 3rd party directory systems as an authentication method.
8.	The solution must support the automatic update of configuration information with minimal user intervention. For example, security taxonomy updates, vendor rule updates, device support, etc.
9.	The solution must support a web-based GUI for management, analysis and reporting.
10.	The solution must ensure all distributed system components continue to operate when any other part of the system fails or loses connectivity. (i.e., management

	console goes off-line all separate collectors still continue to capture logs).
11.	The solution must have an automated backup/recovery process.
12.	The solution must automate internal health checks and notify the user when problems arise.
13.	The solution must provide the ability to deliver multiple dashboards that can be customized to meet the specific requirements of different users of the system.
14.	The solution must deliver sample dashboards out of the box (i.e. for threat management, compliance management, etc.).
15.	The solution must deliver customizable dashboard widgets that can present relevant security information to the users of the system (i.e. event views, network activity views, incident views, etc.).
16.	The solution must maintain a database of all assets discovered on the network. This asset data must include important information about the asset as learned by the information collected (i.e. system attributes, network attributes, vulnerability state, etc.). The database must provide the ability to edit attributes when they cannot be learned (i.e. department, location, etc.). The user must be able to search this database.
17.	The solution must integrate with other security and network intelligence solutions.
18.	The solution must ensure the integrity of the information collected.
19.	The solution must support a distributed model for correlation such that counters, sequences, identity lookups, etc. are shared across all collectors. (i.e., look for 25 login failures from the same user name followed by a single successful login for that same user name, where events seen by a single collector do not exceed the threshold of 25, but across multiple collectors would exceed the threshold).
20.	The solution must support user extended taxonomy of events and fields. The user must be able to add their own unique event names (i.e., the ability to add in new fields that are not part of the vendors out of the box schema such as a field called “SpecialID from my Custom Application”).
21.	The solution must allow for custom defined tagging of events.
22.	The solution must provide transparent retrieval, aggregation, sorting, filtering and analysis of data across all distributed components.
23.	The solution must leverage passive asset discovery to allow new or possibly unauthorized devices to be profiled and tracked without manually scanning the network.
24.	The solution must display visual traffic profiles in terms of bytes, packet rates and number of hosts communicating. These displays must be available for applications, ports, protocols, threats and each monitoring point in the network. All of these views must support network location specific view such that they can present information from a single location, the entire network or any other defined grouping of hosts

25.	The solution must have a log collection and archive architecture that supports both short-term (online) at a minimum of 90-days and long-term (offline) event storage at a minimum of one year.
26.	The solution must support log archives on 3rd party storage.
27.	The solution must provide capabilities for efficient storage and compression of collected data.
28.	The solution must support industry log collection methods (syslog, WMI, JDBC, SNMP, Checkpoint LEA, etc.).
29.	The solution must provide agent-less collection of event logs whenever possible.
30.	The solution must support long-term access to detailed security event and network flow data. The system must be able to provide access to at least 12 months' worth of detailed information.
31.	The solution must normalize common event fields (i.e. usernames, IP addresses, hostnames, and log source device, etc.) from disparate devices across a multi-vendor network.
32.	The solution must provide a common taxonomy of events.
33.	The solution must provide the ability to store/retain both normalized and the original raw format of the event log for forensic purposes.
34.	The solution must provide the ability to normalize and aggregate event fields that are not represented by the out-of-the-box normalized fields.
35.	The solution must support/normalize event time stamps across multiple time zones.
36.	The solution must provide a real-time event view of monitored information in raw/original as well as processed/parsed format.
37.	The solution must provide near-real-time analysis of events.
38.	The solution must provide long term trend analysis of events.
39.	The solution must provide the ability to aggregate an analyze events based on a user specified filter.
40.	The solution must provide more advanced event drill down when required.
41.	The solution must provide a real-time streaming view that supports full filtering capabilities.
42.	The solution must provide alerting based on observed anomalies and behavioral changes in network and security events.
43.	The solution must support and maintain a history of user authentication activity on a per asset basis.
44.	The solution must roll up all events and network flows into single security incidents.
45.	The solution must identify certain protocols that need to be monitored and controlled, such as tor, telnet, ftp, p2p.

46.	The solution must profile traffic by application type (not well-known TCP port).
47.	The solution must provide reporting on all items available for management via the GUI.
48.	The solution must provide configurable reporting engine for customized report creation.
49.	The solution must support the ability to schedule reports.
50.	The solution must provide templates for the easy creation and delivery of reports at multiple levels ranging from operations to business issues.
51.	The solution must provide ‘canned’ out-of-the-box reports for typical business and operational issues.
52.	The solution must provide ‘canned’ out-of-the-box reports for specific compliance regulations (PCI) and control frameworks including (NIST, and ISO).
53.	The solution must provide a ‘Dashboard’ for quick visualization of security and network information.
54.	The solution must support the automated distribution of reports.
55.	The solution must support the capability to provide historical trend reports.
56.	The solution must support the ability to centrally deliver vulnerability reports.
57.	The solution must support the ability to centrally deliver asset reports.
58.	The solution must have the ability to generate reports on flows and events and to declare higher level aggregation of raw events into meaningful "Security Incidents" worth investigating.
59.	The solution must provide searching & data/log management, including free form search.
60.	The solution must provide alerting based on observed security threats from monitored devices.
61.	The solution must provide the ability to correlate information across potentially disparate devices.
62.	The solution must provide alerting based on observed anomalies and behavioral changes in network activity (flow) data and pre-packaged alerts and method for adding user-defined anomaly and behavior alerts.
63.	The solution must provide alerting based upon established policy. (e.g., IM traffic is not allowed.)
64.	The solution must support weighted alerts to allow for prioritization. Weights must be assignable based on multiple characteristics such as asset type, protocol, application, etc.
65.	The solution must provide the ability to transmit alerts using multiple protocols and mechanisms to other management solutions
66.	The solution must provide UI based wizard and capabilities to minimize false positives and deliver accurate results.

67.	The solution must limit the presentation of multiple similar alerts.
68.	The solution must support the ability to take action upon receiving an alert. For example, the solution should support the ability to initiate a script or send an email message.
69.	The solution must support the ability to correlate against 3rd party security data feeds (i.e. geographic mapping, known botnet channels, known hostile networks, etc.). These 3rd party data feeds should be updated automatically by the solution.
70.	The solution must support the ability to correlate against 3rd party vulnerability scan results.
71.	The solution must monitor and alert when there is a disruption in log collection from a device. In other words, if logs are not seen from a server in X minutes then generate an alert.
72.	The solution must provide an out of the box mechanism to discover and classify assets by system type (i.e. mail servers vs. data base servers) to minimize false positives associated with poor asset classification.
73.	The solution must support correlation for additive values over time. For example, alert when any source IP sends more than 1GB of data to a single port on a single destination IP in a one-hour period of time.
74.	The solution must provide a mechanism, to optimize rule tuning, which allows for the grouping of similar input values of a correlation rule that can be used by multiple rules. This grouping mechanism should allow for both static groups and groups that are dynamically created by other correlation rules. For example, the user of the system can define a group of banned ports/protocols that should be used across multiple correlation rules that monitor for inappropriate network activity.
75.	The solution must have the ability to correlate on both flows and events within one correlation rule, thus reducing the number of false positives.
76.	The solution must provide correlation in near-real time.
77.	The solution must display visual traffic profiles in terms of bytes, packet rates and number of hosts communicating. These displays must be available for applications, ports, protocols, threats and each monitoring point in the network. All of these views must support network location specific view such that they can present information from a single location, the entire network or any other defined grouping of hosts.
78.	The solution must support application definition beyond protocol and port. The system must support the identification of applications using ports other than the well-known, and applications tunneling themselves on other ports (e.g., HTTP as transport for MS-Instant Messenger should be detected as Instant messenger - not HTTP).
79.	The solution must detect “zero-day” events.
80.	The solution must dynamically learn behavioral norms and expose changes as they occur.
81.	The solution must detect denial-of-service (DoS) and distributed denial-of- service (DDoS) attacks.

82.	The solution must detect and present views of traffic pertaining to observed threats in the network.
83.	The solution must profile traffic by TCP and UDP port.
84.	The solution must support traffic profiling associated with logical network design (e.g., Subnet/CIDR).
85.	The solution must identify network traffic from potentially risky applications (e.g. file sharing, peer-to-peer, etc.).
86.	The solution must be able to profile communication originating from or destined to the internet by Geographic regions in real-time.
87.	The solution must support traffic profiling based on IP addresses, groups of IP addresses, source/destination IP pairs etc.
88.	The solution must provide a mechanism to capture all relevant aspects of a security incident in a single logical view. This view should include relevant events, network activity data, correlated alerts, vulnerability data, etc.
89.	The solution must provide a mechanism to track security incidents across a wide range of relevant attributes (i.e. IP addresses, usernames, MAC address, log source, correlation rules, user defined, etc.). The user must be able to filter incidents along these defined attributes.
90.	The solution must support the following vendor products: (a) Check Point Firewalls (b) Cisco Routers and Switches (c) Cisco Wireless LAN Controllers (d) F5 Application Delivery Controllers (e) InfoBlox DHCP and DNS appliances (f) Symantec Endpoint Protection (g) Symantec Messaging Gateway (on-premise)
91.	The solution must support information collected from Microsoft based servers and end-user systems.
92.	The solution must support information collected from Linux/Unix based servers and end-user systems.
93.	The solution must support information collected from enterprise class database solutions.
94.	The solution must support information collected from commercial applications (i.e. SAP, PeopleSoft, etc.).
95.	The solution must support information collected from proprietary applications.
96.	The solution must support information collected from Directories (i.e. AD, LDAP) products.

97.	The solution must support information collected from Network flows (i.e. Netflow, J-Flow, S-Flow etc.) products.
98.	The solution must support information collected from Network infrastructure (i.e. switches, routers, etc.).
99.	The solution must support information industry leading vulnerability scanners.
100.	The SIEM must support the ability to create custom device support at no additional cost.