CITY OF TORRINGTON

PURCHASING DEPARTMENT
140 Main Street, Room 206
Torrington, CT 06790

Pennie Zucco, Purchasing Agent
Phone: (860)-489-2225
Fax (860)-489-2547
Email: pennie_zucco@torringtonct.org

March 16, 2023

Mayor Elinor Carbone
Members of the City Council

RE: RFP # XSS-018-031023 XDR SECURITY SOLUTION FOR CITY

The City of Torrington received four (4) proposals pertaining to the eXtended Detection and Response Security Solution for the City. A non-responsive proposal received disqualified one vendor.

Xcitium Inc. **Bloomfield. CT**	**$ 22,200.00**
Vancord Milford, CT	$151,529.00
Advanced Corporate Networking Digital Back Office Milford, CT	$7,568.00 – Option 1 $16,018.05 – Option 2

It is the recommendation of Gerry Crowley, IT Director and the Purchasing Agent that City Council authorize the Mayor to award the purchase of the XDR Security Solution for the City of Torrington to Xcitium, Inc., Bloomfield, NJ. The cost for this project is $22,200.00 and to have the Mayor act on the behalf of the City regarding the execution of the contract and it administration.

Funding of this project will be through the IT Software GL account,

Thank you for your consideration in this matter.

Pennie Zucco
Purchasing Agent

cc: G. Crowley

CITY OF TORRINGTON

INFORMATION TECHNOLOGY
City Hall
140 Main Street
Torrington, CT 06790

Phone: (860) 489-2305
www.torringtonct.org

Memorandum

TO: Mayor Carbone

FROM: Gerry Crowley

DATE: March 16, 2023

RE: XDR Security Solution for City

Mayor,

The IT Department is requesting the City Council's approval to acquire the Xcitium M(X)DR Complete security solution. This advanced product offers a wider range of security features than our current EDR solution, enabling the City to detect and respond to security alerts and incidents more efficiently and effectively. In addition to safeguarding endpoints, the solution also provides protection for network and cloud services, ensuring comprehensive security coverage across all areas of operation.

The supporting RFP documentation will be provided by the Purchasing Department

Thank you;

Gerry Crowley

CC: Pennie Zucco, Purchasing Agent

City of Torrington

Bid Name XDR Security Solution for City

Date of Opening 3/16/23

Bid Number XSS-018-63023

Time of Opening 11:00am

VENDOR	BID BOND	NON-COLLUSION	BID AMOUNT	ADDENDUM
Tyler One Tyler Drive Yarmouth, Maine 04096	N/A	✓	$34000.00 product licensing	#1
xelium Inc. 200 Broadacres Dr. Bloomfield, NJ 07003 ck#96054 13931	$1100.00	✓	$17,400.00 product licensing $2,000.00 installation + set up $2800.00 prof. services	#1
Vancord/Krystal Racine 223 Barrett Hill Rd Brooklyn, CT 06234 ck#982 7333081	$8,450.00	✓	$39,440.00 product licensing $94,800.00 insta prof. services $17,289 installation + set up	#1
Digital BackOffice 192 Naugatuck Ave Milford, CT 06460 ck#1341013920	$580.00	✓	Option 1. Product licensing - $5567.00 DBO Network - 2,066.00 option 2. Product licensing - 59,794.10 Palo Alto Premium - 6,218.95	#1

CITY OF TORRINGTON
REQUEST FOR PROPOSAL

RFP # XSS-018-031023 XDR SECURITY SOLUTION FOR CITY

Bid Opening: March 10, 2023 Time: 11:00 AM Location: City Hall, 140 Main St., Room 206, Torrington, CT

Bid Bond or Certified Check required with bid: 5%

Performance Bond required if awarded bid: N/A

<mark>SUBMIT AN ORIGINAL AND (3) THREE EXACT COPIES.</mark>

The City of Torrington reserves the right to accept or reject any or all bids or any portion thereof, to waive technicalities, and to award the contract as will best serve the public interest.

Omit State and Federal Taxes.

All prices must be F.O.B.: Destination (Torrington) unless otherwise requested.

Dated in Torrington: February 23, 2023   Purchasing Agent _____
                                                                    Pennie Zucco

Item
REQUEST FOR PROPOSAL FOR EXTENDED DETECTION AND RESPONSE (XDR) SECURITY SOLUTION FOR CITY OF TORRINGTON.

The Purchasing Agent is authorized to offer City based bidders that exceed the lowest bid by up to 6%, the opportunity to match the lowest bid. A City based bidder within the 6% differential who agrees to accept the amount of the lowest bid will be awarded the bid. When multiple City based bidders agree to accept the amount of the low bid then the City based bidders will be invited to submit a new bid, not to exceed the low bid. The bid will then be awarded to the lowest responsive, responsible bidder.

Bidder: Xcitium, Inc

Address: 200 Broadacres Drive, 2nd Floor

(Signed By) *Megan Tolmie*   Title: Account Executive

Name (please print) Megan Tolmie   Date: 3/6/23

Phone: 208-358-4562   Fax: E-Mail: megan.tolmie@xcitium.com

Federal Tax Identification Number: (FEIN) 20-5583179

Comments: The 5% Bid Bond will be delivered seperately due to remote working constraints.

INSTRUCTION TO PROPOSERS

Sealed bids will be received by the Purchasing Agent, Room 206, 140 Main St., Torrington, CT until the time and date specified on the cover sheet and opened thereafter in the Purchasing Department, Room 206. Bids received later than the date and time specified will not be accepted. In the event of the closure of City Hall, proposals will be opened on the following business day that City Hall is opened. Amendments to or withdrawal of any section of the submitted bid received later than the time & date set for the bid opening will not be considered. Bid proposals must remain in effect for a minimum of 30 days unless otherwise noted elsewhere in the bid specifications.

BID DOCUMENTS: are available upon receipt of this invitation (if not attached) over the Internet at the City's web site: www.torringtonct.org UNDER "Open Bids". Adobe Acrobat reader is required to view this document. If you do not have this software you may down load it for free from Adobe at http://www.adobe.com. Businesses without internet access may contact the Purchasing Department at 860-489-2224 for a copy of the bid documents.

NONAPPROPRIATION: All funds for payment by the City under this contract are subject to the availability of an annual appropriation for this purpose by the City. In the event of non-appropriation of funds by the City Council of the City of Torrington for the goods or services provided under the contract, the City will terminate the contract, without termination charge or other liability, on the last day of the then-current fiscal year or when the appropriation made for the then-current year for the goods or services covered by this contract is spent, whichever event occurs first. If at any time funds are not appropriated for the continuance of this contract, cancellation shall be accepted by the Seller on thirty (30) days prior written notice, but failure to give such notice shall be of no effect and the City shall not be obligated under this contract beyond the date of termination.

FEDERAL PROCUREMENT: Any procurement made pursuant to a federal award or subject to reimbursement, in whole or in part, with federal funds must comply with the City of Torrington's purchasing procedures, State law and the applicable Federal Procurement Requirements, including 2 CFR § 200.322 ("Procurement of recovered materials"), 2 CFR § 200.323 ("Contract cost and price"), 2 CFR § 200.324 ("Federal awarding agency or pass-through entity review"), 2 CFR § 200.325 ("Bonding requirements"), and 2 CFR § 200.326 ("Contract provisions"). In the event of any conflict between Town, State, or federal requirements, the most stringent requirements must be used (See 2 CFR § 200.318.) City employees must comply with funding agency requests for review of technical specifications or procurement documents as provided in 2 CFR § 200.324.

BID BONDS: shall be in the amount of 5% of the total bid made out in favor of the City of Torrington and issued by a Surety company acceptable to the City of Torrington must accompany each bid. A certified check, cashier's check, Treasurer's check, or money order in the same amount may be submitted in lieu of the bid bond. Bids submitted without Certified Check or Bid Bond **will not** be accepted. The City of Torrington will not be held liable for the accrual of interest on any check held by the city in conjunction with this bid. All checks or bid bonds will be refunded to the unsuccessful bidders after award of the bid by the City Council. The deposit check or Bid Bond of the successful bidder will be held in escrow until such time as the city determines that the bidder has or will meet their obligations as stated by the bid. If the bidder fails or refuses within a reasonable time after due notice that the contract has been awarded to him, to execute the same, an amount representing a loss to the city by reason of such failure shall be retained and paid into the city treasury.

REPLIES: whether bid or no bid, submittal must have the bid number clearly identified on the outside of the envelope. Bidders not marking the envelopes with the Bid number and date/time of opening on the envelope will have no recourse against the City of Torrington or its employees. Such bidders run the risk of the bid being opened prior to the scheduled Bid Opening time. Once opened such bids are public record. Any alleged oral agreement made by a bidder or contractor with any agency or employee of the City of Torrington will be disregarded.

FREIGHT: Prices quoted shall be net delivery **F.O.B. Torrington, CT.** All bid prices must include prepaid delivery, assembly, and/or installation (ready for operation and/or use) of all equipment and/ or materials to the individual locations(s) as designated by the Purchasing Agent. All bid prices are to be submitted on the sheets provided on this bid. Quantities and pricing are to be listed in accordance with these sheets.

QUESTIONS: Request for interpretation of any portion of the bid may be made to the Purchasing Agent: Voice 860/489-2225, Fax 860/489-2547 and email: pennie_zucco@torringtonct.org. All bidders questions pertaining to the contract specifications and plans under this contract shall be placed in writing and addressed to: City Purchasing Agent, 140 Main Street, Room 206, Torrington, CT 06790; Any Fax or email shall be followed up with a telephone call to verify receipt. Bidders should check the web site for addendums/updates 48 hours prior to the bid opening.

In the event of receipt of identical bids as to offerings, delivery, service, content, price, etc., the bid will be awarded in accordance with the information contained in the bid document, based on first received as to date and time of receipt of the bid.

EXPARTE COMMUNICATION: Please note that to insure the proper and fair evaluation of a bid, the City of Torrington prohibits exparte communication (i.e., unsolicited) initiated by the Bidder to a City Official or Employee evaluating or considering the bids prior to the time a bid decision has been made. Communication between Bidder and the City will be directed in writing to the Purchasing Agent only. The Purchasing Agent will obtain the information or clarification needed. Exparte communication may be grounds for disqualifying the offending Bidder from consideration or award of the bid and repeat offenders may be disqualified from future bids.

NON-COLLUSION STATEMENTS: In order for bids to be considered, a non-collusive statement must be submitted with the bid. A sample non-collusive bid statement is attached. Bidders may elect to submit their own notarized non-collusion statement. **NOTE:** Documents must be signed before and sealed by a Notary Public. Only documents bearing a notary seal will be accepted.

CONDITIONAL, QUALIFIED OR NON-RESPONSIVE BIDS/PROPOSALS: All bids/proposals shall be submitted in the form and manner as indicated by the bid documents and bid forms. Any proposal which is not submitted in the form and manner indicated by the bid

documents or which contains information, statements, conditions, or qualifications which place conditions or qualifications on the proposal submittal for purposes of making an award, or which alter any proposal terms, conditions, specifications, or forms, which has not been previously approved by written addendum from the Purchasing Agent, or which does not meet legal requirements, shall be declared as a qualified, conditional, or non-responsive proposal and shall be rejected without further consideration. Any proposal response that does not fully respond to and comply with all detailed specifications or requests for information including execution of proposal forms, may be declared "non-responsive" and recommended for rejection. The City of Torrington shall not be responsible for any errors or omissions of the respondent.

UNBALANCED BIDS AND/OR EXCESSIVE LINE ITEM PRICES: The City reserves the right to reject any bids in which unit prices, in the sole opinion of the City, are unbalanced. In addition, where the City has decided to make an award, it further reserves the right to non-utilize a particular line item that in the sole opinion of the City is excessively priced, and reserves the right to obtain that item from another source.

CONTRACT: A response to an Invitation To Bid is an offer to contract with the City of Torrington based upon the terms, conditions, and specifications contained in the City's ITB. Bids do not become contracts unless and until executed by the City, eliminating a formal signing of a separate contract. For that reason, all of the terms and conditions of the contract are contained in the ITB, unless any of the terms and conditions are modified by an ITB Amendment, a Contract Amendment, or by mutually agreed terms and conditions in the contract documents.

TAXES: Omit all State and Federal taxes from the bid. The City of Torrington is exempt from the payment of taxes imposed by Federal government and/or the State of Connecticut.

OWNERSHIP OF DOCUMENTS: All documents, including drawings, plans, specifications, videotapes, or other documents or maps prepared by a contractor pursuant to any agreement arising from this bid shall become the property of the City of Torrington upon completion of the project or any termination of the project prior to the completion of the project.

LEGALITY: All bid offers for commodities, work, materials, or equipment hereunder shall comply in every respect with the laws, specifications and requirements of the State of Connecticut and the Federal government. Contractor will comply with the provisions of the Connecticut Fair Employment Practices Law.

LANGUAGE DISPUTES: Any disputes over the interpretation and/or meaning of any individual terms, conditions, and/or language within this Request for Bid/Proposal document shall be resolved by and at the sole discretion of the City Purchasing Agent in a manner that is in the best interest of, and best advantage to, the City of Torrington, provided any such interpretation shall be reasonable. In the event that an individual term, condition, and/or language/wording is determined at any time, including after award, by the City Purchasing Agent to be "not applicable at all" to this contract, then the term, condition, and or language/wording may be disregarded, even though an addendum is not issued. However, if the Purchasing Agent determines that the term, condition, and/or language/wording "is applicable in part", then the term, condition, and/or language/wording will apply to the degree applicable, even though an addendum is not issued.

INDEMNIFICATION: The Contractor shall save the City of Torrington, its agents or employees, harmless from liability of any kind for all claims of labor payments and materials furnished for this work, and for use of any copyrighted or uncopyrighted composition, secret process patented or unpatented invention, article or application furnished or used in the performance of the contract of which the Contractor is not the patentee, assignee, or licensee. To the fullest extent permitted by law, The bidder shall indemnify and hold harmless the Municipality, its officers, agents, servants and employees from and against all liability, claims, damages, losses and expenses including attorney's fees arising out of or resulting from the performance or lack of performance of the work, provided that any such liability, claim, damage, loss or expense is (a) attributable to bodily injury, sickness, disease or death, or to injury to or destruction of tangible property, including the loss of use resulting hereto from and (b) is caused in whole or in part by any negligent act or omission of the Bidder, any Subcontractor, anyone directly or indirectly employed by any of them or anyone for whose acts any of them are liable.

In any and all claims against the Municipality, its officers, agents, servants and employees by any employee of the Bidder, any Subcontractor, anyone directly or indirectly employed by any of them or anyone for those acts any of them may be liable, the indemnification obligation under these sections to be limited in any way by any limitation on the amount or type of damages, compensation or benefits payable by or for the Bidder or any Subcontractor under Worker's Compensation Acts, Disability Benefit Acts or other employee benefit acts.

The successful bidder, vendor, and/or contractor must protect all property of the City of Torrington (i.e. all floors, furniture, grass, land, etc.) from injury or other damage. Any damage so caused must be repaired by contractor/vendor at his/her own expense. At the completion of work, the vendor and/or contractor must remove from the premises all surplus materials and all debris created by same. The premises must be left in a broom-clean and finished condition acceptable to the owner or its agents. Successful bidder will furnish adequate protection from damage for all work and to repair damage of any kind; for which he or his workers are responsible, to the premises or equipment to his own work or to the work of other contractors.

DEFAULT: It shall be understood that a bidder supplying equipment and/or supplies will be considered to be in default if/when they have not delivered the item(s) within the time constraints listed in this document or subsequent purchase orders and/or contract. Bidders providing a service and/or construction will be considered to be in default if/when they have failed to meet the completion date set forth in this document or its subsequent contract and/ or purchase orders and/ or they have ceased work on the project for a period of fifteen (15) working days, cumulative or consecutive.

SUSPENSION AND DEBARMENT: The Purchasing Agent may suspend or debar the right of a vendor to be included on the vendor list and has the authority to reject any bid or response from any suspended or debarred vendors.
Suspension: A vendor may be suspended based on the following:
1) A vendor defaults or fails to fully comply with the conditions, specifications, or terms of a Bid, Quotation, Proposal or Contract with

the City of Torrington.
2) A vendor commits any fraud or misrepresentation in connection with a Bid, Quotation, Proposal, or Contract with the City of Torrington.
3) A vendor is charged by a court with the commission of a criminal offense as incident to obtaining or attempting to obtain a public or private contract or sub-contract, or in the performance of such contract or sub-contract
4) A vendor is charged by a court with the following: embezzlement, theft, forgery, bribery, falsification or destruction of records, receiving stolen property, or any other offense indicating a lack of business integrity or business honesty which currently, seriously, and directly affects responsibility as a City contractor. If charges are dismissed or the vendor is found not guilty, the suspension shall be lifted automatically upon written notification and proof of final court disposition provided by the vendor to the City of Torrington.
5) A vendor becomes insolvent, has proceedings in bankruptcy instituted against it or, compounds its debts or assigns over its estate or effects for payment thereof, or has a receiver to trustee appointed over its property.
6) A vendor's commission of any act or omission to perform act is grounds for debarment.
7) A vendor violates the ethical standards set forth in local, state, or federal law.
8) Any other cause the Purchasing Agent determines to be so serious and compelling as to materially and adversely affect responsibility of a vendor as a City contractor, including but not limited to suspension by another government entity

Debarment: A vendor may be permanently debarred for the following:
1) Default or failure to fully comply with the conditions, specifications, drawings, or terms of a bid, proposal, or contract with the City of Torrington twice in any three-year period.
2) Conviction of or judgment obtained in a court for commission of those offenses in connection with the vendor's commercial enterprise stated sections 3) or 4) of suspension section listed above. If the conviction is reversed through the appellate process, the debarment shall be removed upon written notification and proof of final Court disposition from the vendor to the City of Torrington.

TRADE NAME REFERENCES: Any and all references to trade names, types, styles, model numbers, stock numbers or catalogs are intended to be descriptive only and not restrictive. The intention is to indicate to bidders the type and quality of the articles and or materials that will be satisfactory. When reviewing the information, it is the responsibility of the prospective bidder to inform the City of Torrington of any discrepancy that is found (i.e. number listed does not fit item description) Bids received on other makes or models with reference to other catalogs will be considered. The bidder is to clearly state in his bid exactly what he intends to furnish and to furnish with his bid a cut or illustration or other descriptive matter that will clearly indicate and give specification as to the product he/she proposes to furnish. Where a bid is offered on an item other than the trade standard used in the specification the item should be identified on the bid form by entering the MAKE, TRADE NAME AND MODEL NUMBER. It is understood that any substitute and/or alternate that might be offered are guaranteed by the bidder to be of equal or better quality than is referenced in the bid. The item(s) must be equivalent as to function, basic design, type and quality of material, method of construction and any required dimensions. It shall be further understood that during original as well as subsequent shipments spot checks will be performed to insure that the items received are in fact the items offered in the bid. When received, should items/materials prove to be different from what was bid in any way, the bidder agrees to the return of the items and agrees to supply correct items (per bid specifications) at the bidders expense. In the event this return action is required, it is understood the bidder may be subject to removal from the city's approved bidder's list. Bidders are cautioned that surplus, seconds, factory rejects, floor samples, close outs or distressed items are not acceptable and shipments of substitutions, defective or shop-worn equipment will be returned for a full refund at the vendor's expense.

QUANTITY: The quantities and/or materials listed in the specifications/bid sheets may be increased or decreased by the City of Torrington or its designated representative based on actual need at the time the purchase orders are placed.

QUALITY: The City of Torrington reserves the right to reject any proposal in whole or in part offering equipment and/or materials and/or services that in its or its agent's opinion does not meet the quality standards desired. Such decision is final and not subject to further recourse by the bidder.

SAMPLES: forwarded by the bidder will be returned to the bidder at his request and expense. Requests for return of samples must be submitted in writing at the time the sample is given to the City of Torrington or its representative. Samples not returned to the bidder will be disposed of at the discretion of the City of Torrington or its designated representative. Large pieces of equipment submitted for evaluation and inspection are to be picked up by the bidder within 30 days of the bid opening date. Items remaining after 30 days will be discarded.

AWARD: It is the intent to award this bid in its entirety to one bidder, however, the City reserves the right to award the bid line item by line item if it is deemed in its best interest to do so. In addition, bidders are advised that should budgetary constraints dictate, part, and/or all the items in this bid may be rejected. This decision shall be considered final and not subject to recourse by the bidder. In determining the lowest or highest responsible bidder, the City reserves the right to consider, in addition to price, the compatibility, quality, cost of maintenance and availability of parts, experience and/or past performance of the bidder, sufficiency of the financial resources of the bidder as relates to the offerings as well as the ability of the bidder to provide future maintenance and service.

Documents previously submitted to the City of Torrington will not be considered as satisfying submission requirements for this bid.

No bidder can claim any contract rights by virtue of bidding alone. Awarding of the contract means actual written notice by letter and a properly executed purchase order to the bidder or bidders to whom the bid has been awarded.

OPTION TO RENEW: This contract may be extended for four (4) additional one (1) year periods, provided all terms and conditions remain in full force and effect except for the contract period being extended. This option, if exercised, is to executed in the form of a letter of agreement, to be issued no later than 30 days prior to the expiration of the then current contract period. This option to renew requires the mutual agreement of both parties. Refusal by either party to exercise this option to extend, will cause this contract to expire on the original or mutually agreed upon date. The total period of this contract, including all extensions as a result of exercising this option, will not exceed a maximum combined period of five (5) years.

BONDS:

Performance Bond: The Contractor, when awarded the Bid, must submit within 10 days of the bid award, and before beginning the work or signing a contract, a Performance Bond amounting to one hundred percent (100%) of the total amount of the bid. Said performance bond must be in favor of the City of Torrington and executed by a surety company authorized to do business in the State of Connecticut. The City of Torrington reserves the right to retain the Bid Bond or Certified Check on bids below $25,000.00 as a Performance Bond. On bids of $25,000.00 or more the Performance Bond may be furnished in the following manner: Performance Bond, Surety Bond, Certified Check or Bank Check.

Maintenance Bond: The contractor, upon signing a contract and before beginning the work must submit to the Purchasing Agent a Maintenance Bond to guarantee that if defects in either labor or materials becomes evident within one year after completion and acceptance of work will be fixed at no cost to the City of Torrington. The maintenance bond may be included as a portion of the Performance bond or as a separate bond. If it is issued as a separate bond said maintenance bond must be in favor of the City of Torrington and issued by a surety company licensed and authorized to do business in the State of Connecticut.

Labor and Material Bonds: Per Section 49-41 of the Conn. General Statutes, on Public Works project where the estimate is in excess of $25,000.00, a labor (payment) and material bond must be furnished to the City. Said bonds must be filed with the Purchasing Agent prior to the commencement of work.

Consent for Release of Final Payment: AIA Document G707 & G706, or equivalent, must be signed and returned by the Surety Company before final payment will be released to the contractor.

INSURANCE:

Certificate of Insurance: All insurers shall purchase insurance from an insurance company or companies rated A-V11 or better by A.M. Best Companies lawfully authorized to do business in the State of Connecticut. The insurance provisions set forth below are minimum requirements. In the event the Contractor/City Contract (Project Requirements) specifies additional coverage's and/or amounts of coverage then those set forth below and pertaining to the Contractor's work, then the Contractor shall provide the coverage's and/or amounts in accordance with the Project Requirements. Proof of proper insurance coverage, Workers Compensation Insurance, Liability and Property damage, and Vehicle Insurance shall be filed with the City of Torrington Purchasing Agent within 10 days after the award of the bid. The Certificate of Insurance must name the City of Torrington, 140 Main St., Torrington, CT, its subsidiaries, employees, volunteers, directors & officers as the "Additional Insured" and filed with the Purchasing Agent prior to commencement of work. Renewal Certificates of Insurance must be mailed to the Purchasing Agent 10 days prior to the expiration of the required coverage. Such insurance will protect the Contractor from claims which may arise out of or result from the Contractor's operations under the Subcontract and for which the Contractor may be legally liable, whether such operations be by the Contractor or by a Sub-Contractor or by anyone directly or indirectly employed by any of them, or by anyone for whose acts any of them may be liable. Contractor, and any Sub-subcontractors engaged by the Contractor, shall obtain the following insurance:

Workers' Compensation Insurance: For all work performed pursuant to this contract, Contractor shall maintain Workers' Compensation Insurance, including coverage for all executive officers, sole proprietors and partners, and other similar employee benefits in the amount required by all applicable statues, law, regulations or acts. Such Workers' Compensation Insurance must list on Item 3A of the policy Information Page "Part One of the policy applies to the Workers' Compensation Law of **the state Connecticut"** and provide a Waiver of Subrogation endorsement (NCCI form WC 00 03 13 or its equivalent) that prohibits the insurance company from enforcing subrogation and recovery rights against the City, its subsidiaries, employees, volunteers, directors and officers. If work is to be performed over or adjacent to navigable waterways, the Workers' Compensation Insurance shall contain the United States Longshore and Harbor Workers' Act Endorsement (NCCI Form WC 00 01 06 or its equivalent). In case any class of employees or subcontractors is engaged in hazardous work under the contract at the site of the work is not protected under the Workman's Compensation statute, the contractor shall provide Workman's Compensation Insurance for the protection of employees not otherwise protected.

Liability Insurance: The Contractor shall take out and maintain for the life of the contract, adequate public liability insurance insuring against liability to persons not employed by him in an amount of not less than $1,000,000.00 for injuries, wrongful death to any one person and subject to the   limit for each person in an amount of not less than $2,000,000.00 on account of one accident and property damage insurance in an amount of not less than $1,000,000.00.

Vehicle Insurance: The Contractor shall take out and maintain for the life of the contract, adequate automotive/truck or other vehicle insurance with minimum coverage of $1,000,000.00 each for both liability and under insured and uninsured motorist as well as any other coverage required by the State of Connecticut or requested by an official of the City of Torrington as relates to the contract.

Additional Security: The City of Torrington reserves the right to require successful bidders to enter into and such security arrangements as are deemed necessary to protect the City of Torrington, its property and goods.

PERMITS: The successful bidder agrees to obtain all work/building permits as might be required. The cost of obtaining such permits is the responsibility of the bidder. The City of Torrington reserves the right to waive local permit fees. In addition, it shall be understood that where property lines are to be considered, bidders are to verify said lines and measurements with proper City Officials prior to commencement of work.

It is to be understood that any/all specifications and/or plans or drawings contained in or developed as a result of the bid process are and shall be presented subject to the approval of the City of Torrington planning, zoning and building officials and that awards made prior to said approval are subject to cancellation.

PREVAILING WAGE: When the State of Connecticut Prevailing Wage Rate is applicable to the bid, the successful bidder must submit a Certified Payroll Record prior to any request and/or invoice for payment.

CITIZENSHIP: Each employee of the Contractor shall be a citizen of the United States or an alien who has been lawfully admitted for

permanent residence as evidenced by an Alien Registration Receipt Card. The Contractor agrees not to employ any person undergoing sentence of imprisonment except as provided by Public Law 89-176, September 10, 1065, (18 USC 4082)(c)(2).

SAFETY:

Machine and/or Equipment Hazard Assessment and Safety Training: Upon delivery of machines and/or equipment, suppliers are required to provide to the end-user employees, at no additional charge, a training session that will emphasize hazard awareness and assessment and the safe use of such machinery/equipment.

Occupational Safety and Health Act of 1970: Seller shall warrant that the machinery, equipment or other materials covered hereby shall upon delivery to the City of Torrington, be in compliance with the standards required by said Act and any updates as pertain to or reference said Act as well as the standards required by comparable State and local laws, if any, for such machinery, equipment or other materials in effect at the time of delivery.

Machines and/or Equipment Lockout/Tagout: In an effort to comply with OSHA's final rule on the control of hazardous energy sources, vendors must warrant that any and all machines and/or equipment as is covered under this bid will be supplied and/or installed equipped with lockout/tagout devices as prescribed by OSHA.

Toxic Substance Control Act (PL94-469): Seller warrants that each and every chemical substance constituting or contained in the products sold or otherwise transferred to the City of Torrington under this bid and subsequent purchase orders is not on the list of prohibited chemical substances compiled and published by the Administrator of the Environmental Protection Agency pursuant to Act PL94-469 and are otherwise in compliance with said Act.

Hazardous Materials: Any materials required by this bid and subsequent purchase orders that are hazardous under federal, state, or local statute, ordinance, regulation, or agency order will be packaged, labeled, marked and shipped by the seller to comply with all federal, state and local regulations then in effect including but limited to the provisions of the Hazardous Materials Transportation Act and Regulations promulgated thereunder and will further comply with any special requirements and any policies and procedures of the City of Torrington relating to the purchase of hazardous materials as might be noted on subsequent purchase orders or otherwise communicated to seller in writing.

Material Safety Data Sheets: Shall be provided by the Seller upon delivery to the City of Torrington of any goods having constituents listed in the following references - OSHA 1910, ACHIG Current Threshold Values, DOT HazMat Table 49, IARC Carcinogen List, National Toxicology Program Carcinogen List, and/or Radioactive Materials. These Material Safety Data Sheets must be consistent with and include information required by the OSHA Hazard Communication Standard published as 29 CFR 1910.1200, as the same may be amended or supplemented from time to time.

Asbestos: Bidders are advised that asbestos-containing material may be located in the boiler rooms, pipe tunnels, storage areas and various portions of City buildings. Before proceeding on any contractual work on City buildings or their interiors, it is mandatory that bidders familiarize themselves with the asbestos-containing material and that said material be considered as a health hazard and all precautionary measures according to the Ahera Rules & Regulations be observed. It is the bidder's responsibility to notify all employees and/or subcontractors of this notification.

SUB-CONTRACTORS: The successful bidder shall not employ any subcontractor to fulfill any of the duties herein specified without express, prior written approval of the City of Torrington or its designated agent.

EEO: The successful bidder shall provide any/all additionally required, affirmative action statements, fair employment plans and non-discrimination programs and statement as might be required by the City of Torrington. In connection with the execution of this bid, subsequent purchase orders and/or contracts, the seller shall not discriminate against any employee or applicant for employment because of age, race, religion, color, sex or national origin. Bidders must comply with all rules & regulations of the Department of Labor with regard to Equal Employment Opportunities as pertains to municipalities.

TERMINATION OF CONTRACT: Any contract entered into by the City and the successful bidder shall provide that the City may terminate the contract upon thirty (30) days notice to the bidder.

The City of Torrington reserves the right to award or reject any or all bids, or any portion thereof, to waive technicalities, to award the contract to a bidder other than the lowest bid and to award the bid and/or contracts to one or more bidders submitting essentially identical proposals and, that in the city's judgment, will best serve the public interest.

The terms and conditions of these "Instructions to Bidders" are made a part this bid.

NON-COLLUSION AFFIDAVIT

STATE OF __Idaho__ COUNTY OF __Ada__

I, __Megan Tolmie__ , being first duly sworn, deposes and says that:

1. I am __an employee__ of __Xcitium, Inc__ , the Bidder
    that has submitted the attached Bid for " __XDR Solution for the City__ ";

2. I am fully informed respecting the preparation and contents of the attached Bid and of all pertinent circumstances respecting such bid;

3. Such Bid is genuine and is not a collusive or sham Bid;

4. Neither the said Bidder nor any of its officers, partners, owners, agents, representatives, employees or parties of interest, including this affiant, has in any way colluded, conspired, connived or agreed directly or indirectly with any other Bidder, firm or person to submit a collusive or sham Bid in connection with such Contract, for which the attached Bid has been submitted nor has it in any manner, directly or indirectly, sought by agreement or collusion or communication or conference with any other Bidder, firm or person to fix the price or prices in the attached Bid or of any other Bidder, or to fix any overhead, profit or cost element of the Bid price or the price of any Bidder, or to secure through any collusion, conspiracy, connivance or unlawful agreement any advantage against the City of Torrington or any person interested in the proposed Contract; and

5. The price or prices quoted in the attached Bid are fair and proper and are not tainted by any collusion, conspiracy, connivance or unlawful agreement on the part of the Bidder or any of it agents, representatives, owners, employees, or parties in interest, including this affiant.

(Printed) __Megan Tolmie__

(Signed) __Megan Tolmie__

(Title) __AG__

Subscribed and sworn to before this __7th__ day of __March__ , 20 __23__ .

__Michael Parson__
Notary Public Printed

Notary Public Signature

My Commission Expires __02/01/29__

(Notary Seal)

MICHAEL PARSON
Notary Public - State of Idaho
Commission Number 20230525
My Commission Expires 02-01-2029

NOTE: Documents must be signed before and sealed by a Notary Public. Only documents bearing a notary seal will be accepted.

REQUEST FOR PROPOSAL
RFP # XSS-018-031023 XDR
XDR SECURITY SOLUTION FOR CITY

The City of Torrington is seeking proposals from qualified vendors to provide an XDR (eXtended Detection and Response) security solution to enhance the security posture of our network and protect against cyber threats. The City of Torrington operates a complex network infrastructure that supports critical services for our community, including public safety, utilities, and administrative functions. Given the constantly evolving threat landscape, it is essential that we maintain a robust security framework to safeguard our network and data from external and internal threats.

We are looking for a comprehensive and scalable XDR solution that can provide advanced threat detection, analysis, and response capabilities to protect our infrastructure and sensitive information. The XDR solution should integrate with our existing security systems and be able to provide visibility across our entire network, including on-premises, cloud, and hybrid environments. The proposed solution should also be flexible enough to accommodate future upgrades and changes to our infrastructure.

The City of Torrington seeks to partner with an experienced and reputable vendor that can provide a turnkey solution and professional services, including implementation, training, and support. The vendor should have a proven track record of delivering XDR solutions to government agencies, preferably at the local level. The vendor should also demonstrate compliance with industry standards and regulations, such as NIST, CIS, HIPAA, and PCI-DSS.

We invite proposals from vendors who have the experience, expertise, and resources to provide a comprehensive XDR solution that meets our security needs. Proposals should include detailed descriptions of the proposed solution, pricing, implementation plan, and support and maintenance services. Proposals should also demonstrate how the proposed solution will help us achieve our security goals and comply with relevant regulations.

We look forward to receiving proposals from qualified vendors and partnering with a vendor that can help us enhance our security posture and protect our critical services and information.

The deadline for bid submittals is **Friday, March 10, 2023 at 11:00 AM**. Proposals shall be submitted to the Purchasing Department, City Hall, 140 Main Street, Room 206, Torrington, CT 06790. One original and three (3) exact copies shall be placed in a sealed envelope and clearly marked on the outside of the envelope including all outer packaging, such as DHL, FEDEX, UPS, etc.: **"RFP # XSS-018-031023, XDR SECURITY SOLUTION FOR CITY"** and must bear the Name and address of the bidder. Proposals received after the closing date and time shall be rejected and returned unopened. In the case where City Hall is closed for weather related or some other emergency related circumstance, then submittals shall be due the next day when City Hall reopens for business, no later than 11:00 AM on that day. The City will not be liable for any costs incurred in the preparation of the response for this Request for Proposal. All proposal submissions and materials become property of the City and will not be returned. Once opened such bids are public record. Vendors mailing bids should allow for normal delivery time to ensure timely receipt of their bids. The City of Torrington shall not be held responsible for lost or misdirected bids. **No faxed or e-mailed bids will be accepted.**

Deadline for questions is **Thursday, March 2, 2023 by 12:00 NOON.** Submit all questions to Gerry Crowley, IT Director, gerry_crowley@torringtonct.org. Questions determined to be of interest to all prospective bidders will be posted as an addendum on the City and State websites. It is the vendor's responsibility to check these websites 48 hours before the closing date for addenda's. All information given by the city except by written addendum shall be informal and shall not be binding upon the city nor shall it furnish a basis for legal action by any Proposers against the City.

Any alleged oral agreement made by a bidder or contractor with any agency or employee of the City of Torrington shall be disregarded.

All proposals must include the bidder's name and be signed by a responsible officer or employee of the vendor submitting a proposal. The vendor shall provide at least three (3) references of companies or agencies that have purchased similar equipment from vendor.

This RFP does not commit the City of Torrington to select any vendor or enter into any contract agreement. The City of Torrington reserves the right to request additional information from some or all bidders. The City of Torrington reserves the right to accept any RFP deemed in the best interests of the City of Torrington.

The information provided herein is not intended to and shall not bind the City of Torrington to any of the statements or assumptions set forth herein.

Responses must set forth accurate and complete information for each of the items listed below. At the City's discretion, failure to do so could result in disqualification.

Any contract entered into by the City and the successful bidder shall provide that the City may terminate the contract upon thirty (30) day notice to the bidder.

All proposals will be considered valid for a period of ninety (90) days. The successful bidder shall not withdraw, cancel or modify their proposal.

The bidder hereby acknowledges receipt of and agrees this submittal is based on the RFP and the following addenda(s). Failure to indicate receipt of addenda(s) may result in the bidder being rejected as nonresponsive.

ADDENDUM #__1____ DATED _3/3/23_____ ADDENDUM _____ DATED_____

ADDENDUM #_____ DATED_____ ADDENDUM _____DATED_____

ADDENDUM #_____DATED_____ ADDENDUM _____DATED_____

(If additional addenda are issued, attach a complete listing of these addenda when submitting this bid.)

The City of Torrington reserves the right to award or reject any or all bids, or any portion thereof; to waive technicalities; to award the contract to a bidder other than the lowest bid, and to award the bid and/or contracts to one or more bidders submitting essentially identical proposals and, that in the city's judgment, will best serve the public interest.

AN AFFIRMATIVE ACTION/EQUAL OPPORTUNITY EMPLOYER
MBE'S WBE'S AND SBE'S ARE ENCOURAGED TO APPLY

REQUEST FOR PROPOSAL
RFP # XSS-018-031023
XDR SECURITY SOLUTION FOR CITY

1. **INTRODUCTION:**
The City of Torrington (City) is seeking proposals for an XDR (eXtended Detection and Response) security solution to enhance the security posture of our network and protect against cyber threats.

2. **BACKGROUND/EXISTING INFRASTRUCTURE**
The City has a full time staff of four technology professionals supporting approximately ~280 users on ~290 endpoints. The City operates a multi-domain network that is comprised of Microsoft Windows desktops, virtualized on-premise Windows servers and cloud-based systems. The City employs a Microsoft 365 GCC tenant in a hybrid configuration for collaboration, email, and file storage. The City currently utilizes an EDR solution for EPP.

3. **SCOPE OF SERVICES**
The City is seeking a qualified vendor to provide a unified cybersecurity solution capable of providing real time threat detection, analysis and protection from current and emerging threats for on-premise endpoints and cloud resources and across the data network. The ideal solution provides protection across the entire technology stack utilizing automation to coordinate detection, response, and remediation.

Vendor shall provide the following as part of the product implementation:
- Vendor shall provide training for technology staff on all system interfaces and their respective functionality;
- Establishing systems baseline, platform tuning, data ingestion configuration, API connector configuration;
- Playbook development, configuration and implementation, activation of incident response plans;
- Any equipment provided by the vendor as part of solution will be new hardware and currently manufactured and under warranty;
- The vendor shall be responsible for all system/platform maintenance, upgrades, and hardware replacement for the provided solution.

4. **EVALUATION FACTORS**
After receipt of Proposals, the City will use the following criteria in the selection process:
- Qualifications of Solution/Vendor
- Vendor's incident response and remediation capability.
- Ease of Solution integration with City technology stack
- Product Cost
- References/Experience

5. **SUBMITTALS**
Proposal submissions shall be submitted to the Purchasing Department and shall include the following documents:
1. Acknowledgement of any addenda on page 9
2. Pricing Schedule (Exhibit A).
3. The Terms acceptance form (Exhibit B) signed by an authorized agent of the company.
4. Reference Sheet (Exhibit C)
5. XDR Solution Questionnaire (Exhibit D, pgs. 15 – 21)

All Required forms – non-collusion affidavit, bid bond, references, etc.

The City of Torrington reserves the right to award or reject any or all bids or any portion thereof, to waive technicalities, to award the contract to a bidder other than the lowest bid and to award the bid and/or contracts to one or more bidders submitting essentially identical proposals and, that in the city's judgment, will best serve the public interest.

AN AFFIRMATIVE ACTION/EQUAL OPPORTUNITY EMPLOYER
MBE'S WBE'S AND SBE'S ARE ENCOURAGED TO APPLY

EXHIBIT A
PRICE SHEET
RFP # XSS-018-031023
XDR SECURITY SOLUTION FOR CITY

(XDR) eXtended Detection and Response Solution Price Summary	
Item (290EP)	**Cost**
Product Licensing	$17,400
Installation & Setup	$2,000
Professional Services	$2,800

EXHIBIT B

REQUEST FOR PROPOSAL
RFP # XSS-018-031023
XDR SECURITY SOLUTION FOR CITY

Acceptance of Terms of this Agreement

Company (Legal Registration)   Xcitium, Inc

Contact Person: Megan Tolmie

Address: 200 Broadacres Drive, 2nd Floor

City/State/Zip: Bloomfield, NJ 07003

Federal Tax Identification Number (FEIN)   20-5583179

Telephone: 208-358-4562   Fax:

E-mail: megan.tolmie@xcitium.com

Authorized Signature *Megan Tolmie*   Title: Account Executive

Name Printed: Megan Tolmie   Date: 3/6/23

It is agreed by the above signed proposer that the signature and submission of this proposal represents the proposer's acceptance of all terms, conditions, and requirements of the proposal specifications, and, if awarded, the proposal will represent the agreement between the parties.

The proposer agrees that the cost of any work performed, materials furnished, services provided, or expenses incurred, which are not specifically delineated in the proposal documents, but which are incidental to the scope, intent, and completion of this contract, shall be deemed to have been included in the prices for the various items scheduled.

EXHIBIT C
XDR SECURITY SOLUTION FOR CITY
RFP # XSS-018-031023

STATEMENT OF REFERENCES

List five (5) references that demonstrate your ability to supply equipment and services included in the scope of the specifications. The City reserves the right to contact each of the references listed for additional information regarding your company's qualifications.

Reference calls made upon request

Reference No. 1
Vendor Name/Email: Chestnut Health Systems
Contact Individual: Jim Edmonds   Phone No: 618-512-1991
Address: 1003 Martin Luther King Jr Dr Bloomington, IL 61701
Contract Amount: $25,000   Year: 2022
Description of products purchased: XDR

Reference No. 2
Vendor Name/Email: Project Enhancement Corporation
Contact Individual: Sean McGrath   Phone No: 240-686-3059
Address: 20300 Century Blvd Germantown, Maryland 20874
Contract Amount: $10,000   Year: 2020
Description of products purchased: XDR

Reference No. 3
Vendor Name/Email: Edge Technologies Inc.
Contact Individual: Jim   Phone No: (512) 733-0110
Address 3000 Joe DiMaggio Blvd. Suite 21 Round Rock, TX 78665
Contract Amount: $3,000   Year: 2021
Description of products purchased: XDR

Reference No. 4
Vendor Name/Email: Ventus Logistics LLC
Contact Individual: Enrique Resendez   Phone No: 210-306-4132
Address: 10205 Crossroads Loop Laredo, TX 78045
Contract Amount: $10,000   Year: 2020
Description of products purchased: XDR

Reference No. 5
Vendor Name/Email: Smokercraft
Contact Individual: Bob Rairigh   Phone No: 574-831-2103
Address: 68143 Clunette St New Paris, Indiana 46553
Contract Amount: $20,000   Year: 2020
Description of products purchased: XDR

EXHIBIT D
XDR SECURITY SOLUTION FOR CITY
RFP # XSS-018-031023

XDR Solution Questionnaire (pgs. 15-21)

INSTRUCTIONS: VENDORS, COMPLETE THE 'SOLUTION' COLUMN IN EACH
SECTION WITH EITHER '**YES**,' '**NO**' OR A VERBAL DESCRIPTION.

XDR - Prevention & Detection		
Attack Type	**Implementation**	**Solution**
The solution must identify malicious files and prevent them from execution, including viruses, trojans, ransomware, spyware, cryptominers and any other malware type.	Signature-based malware protection	Yes
	Local endpoint sandboxing/endpoint emulation	Yes
	Threat intelligence (non-VT feeds)	Yes
The solution must default deny & run virtualized detectionless protection on every unknown file.	Default Deny Security with Default Allow Usability	Yes
	Run unknown files with Virtualization Protection	Yes
	Create Virtual environment for any unknowns	Yes
	Virtualize file system, registry, COM on real endpoints	Yes
The solution must identify and block privilege escalation attacks.	Process monitoring	Yes
The solution must identify and block reconnaissance attacks (scanning).	Network traffic monitoring	Yes
The solution must identify, and block credential theft attempts form either memory (credential dump, brute force) or network traffic (ARP spoofing, DNS Responder).	Memory monitoring	Yes
	User account monitoring (login attempts)	Yes
	Network traffic behavioral analysis	Yes

Attack Type	Implementation	Solution
The solution must identify and block/alert on lateral movement (SMB relay, pass the hash, etc.).	Network traffic monitoring.	Yes
The solution must identify user account malicious behavior, indicative of prior compromise.	Configure user activity policies (policy violation).	Yes
The solution must identify malicious interaction with data files.	Deception via decoy files.	Yes
The solution must identify data exfiltration via legitimate protocols (DNS tunneling, ICMP tunneling).	Network traffic monitoring.	Yes
	File access monitoring.	Yes
The solution must identify and block usage of common attack tools (Metasploit, Empire, Cobalt etc.).	Process monitoring.	Yes
The solution must have an internal protection mechanism against access and manipulation of unauthorized users.	Alert and block upon any tampering or disabling attempt.	Yes

XDR – Monitoring & Control		
Capabilities	Implementation	Solution
The solution must have built-in vulnerability assessment.	Discover missing security updates within systems and applications.	Yes
The solution must provide the means to conduct Inventory Management.	Map and correlate all assets within the environment such as endpoints, servers, installed apps, user accounts and generated periodic reports.	Yes
The solution must provide log collection and retention.	Collect authentication and activity logs, and retain them for the period of time that is required by various regulations.	Yes

The solution must include proactive threat hunting.	Search for malicious presence by known IOC.	Yes
The solution must support the discovery of unattended attack surfaces.	Search for risk susceptible files, processes, network connections and user accounts with unchanged passwords.	Yes

Response Automation: Investigation & Remediation

Capability	Implementation	Solution
The solution must continuously collect data on all the entities and their activities within the environment.	• Process execution (including process tree display). • User login. • Network traffic. • Registry changes. • Installed software.	Ye:
The solution must support the display of entity and activity data.	Search-based on behavioral patterns in all fields of coverage (users, files, machines, and network traffic).	Yes
	Determination of the rules and/or the creation of warning and/or the determination of the risk level, based on a response to the search pattern and in real-time.	Yes
The solution must support dynamic analysis (i.e. sandbox).	Manually submit files to sandbox analysis.	Yes but Containment provides this in real-time, manual submitting is not needed.
The solution must support cross-organization queries.	Search for the occurrence of process/file/network/user activities across all endpoints in the environment.	Yes
The solution must support the means to execute forensic investigation.	• Running process\file. • Machine level. • Memory activities. • Obtain memory dump.	Yes

Capability	Implementation	Solution
The solution must support isolation and mitigation of malicious presence and activity, locally on the endpoint.	Capability of running a coordinated command (such as CMD interface).	Yes
	Running script or a file from a network location or mapping a drive.	Yes
	Shutting down an endpoint and/or a server.	Yes
	Isolation of an endpoint/ server from the network.	Yes
	Deletion of a file (including active run files).	Yes
	Put a file into quarantine (including active run files).	Yes
	Kill a process.	Yes
	Removal and/or deletion of a service/scheduled task.	Yes
	Locking a local user account or a domain user.	Yes
	Zeroing user password.	Yes
	Blocking telecommunications based on destination (domain address or IP address).	Yes
	Disconnection of network cards.	Yes
	Change of IP address.	Yes
	Capability of editing a HOST file.	Yes

	Renewed operation of an end station and/or a server.	Yes
The solution must support isolation and mitigation of malicious presence and activity globally across the entire environment.	Active Directory: disable user, reset password	Yes
	Firewall/proxy: block IP, block domain, block port.	
The solution must support response automation.	Preset response playbooks that are provided off-the-shelf.	Yes
	Customized correlation rules or reporting that are crafted by the operator.	Yes

Infrastructure

Capabilities	Implementation	Solution
The solution must support rapid and seamless installation across all endpoints/servers in the environment.	Require time for deployment across 5000 endpoints.	Yes
The solution must support automated distribution on endpoints/servers that were joined to the environment following the initial installation.	Autonomously discover newly added machines and have the agent installed on them without need of manual configuration.	Yes
The solution must have a light footprint for minimal impact on the endpoint/server performance.	1-5% amount of system CPU processing capacity consumed on each endpoint platform.	Yes
The solution must support all commonly used Operating Systems.	EOL systems: Windows XP\Vista, Server 2003	Yes
	Windows 7 and above	
	Windows server 2008 R2 and above	
	Linux main distros: Fedora, Ubuntu, Debian, Centos, Red Hat, Suse	
	MAC OSX Maverick and above	
	Granular authentication to the UI.	Yes

The solution must support connection to Active Directory.	Deployment to various OU groups with AD.	Yes
The solution must co-exist with all commodity and proprietary software on the endpoints\servers.	Seamless operation of the protected endpoint/server without bluescreens or process crashes.	Yes
The solution must provide full protection for endpoints and servers that are offline from the organization's network.	Threat protection mechanism that do not rely on connectivity to the management server.	Yes
The solution must collect endpoint, file, process, user activity and network traffic in a fully self-sustained manner.	Eliminate the need of manual configuration of rules or policies or reliance of additional devices.	Yes

Operation	
Capabilities	**Solution**
The solution must have the ability to specify a list of alert exclusion rules for the selected objects.	Yes
The solution must support deployment on multiple sites that report into a single management console.	Yes
The solution must have the ability to export the current configuration of the program in order to later be imported to the same or another computer.	Yes
The solution must have the ability to enable/disable certain types of notifications.	Yes
The solution must provide a central collection and processing of alerts in real-time.	Yes
The solution must have the ability to block access to the program settings for end users.	Yes
The solution must provide a central distribution of updates without need of user intervention and of restarting the endpoint/server.	Yes
The solution must have the ability to specify a schedule for downloading updates,	Yes

including the ability to disable automatic update.	Yes
The solution must support the logging of events, alerts and updates.	Yes
The solution must support integration with email infrastructure to notify security personnel in case of alerts.	Yes
The solution must support integration with SIEM products or have the ability to create SIEM-like reports natively.	Yes
The solution must support standardized and customizable reports.	Yes

CITY OF TORRINGTON
Addendum # 1

ADDENDUM 1 IS ISSUED FOR QUESTIONS AND ANSWERS PERTAINING TO THE SECURITY SOLUTION FOR THE CITY OF TORRINGTON

RFP # XSS-018-031023 XDR SECURITY SOLUTION FOR CITY

Date of bid opening: March 10, 2023 **Time:** 11:00 AM **Location:** City Hall, 140 Main St., Room 206, Torrington, CT

<mark>Submit signed addenda with bid.</mark>

The City of Torrington reserves the right to accept or reject any or all bids or any portion thereof, to waive technicalities, and to award the contract as will best serve the public interest.

Dated in Torrington: 2/3/2023   Purchasing Agent _____
                                                                          Pennie Zucco
Authorized Representative ___ Megan Tolmie _____

Authorized Signature _Megan Tolmie_____

Company name _Xcitium, Inc_____

Address _200 Broadacres Drive, 2nd Floor_____

Email _megan.tolmie@xcitium.com_____

Fax _____ Phone _208-358-4562_____

Federal Tax Identification Number: (FEIN) _20-5583179_____

Questions/Answers 2/3/2023

Q1) Is the City looking to have the solution monitored by a 24x7x365 Security Operations Center?
A1) Yes

Q2) How will the contract term be determined for this project?
A2) The contract terms will be discussed with the awarded vendor.

Q3) Does the City have a requirement for services to be hosted in government assessed clouds such as Azure for Government or AWS Gov Cloud?
A3) No, there is no requirement for the vendor's product to be hosted in the clients cloud service(s).

Q4) Please describe your WAN topology and any physically or VPN connected entities.
A4) WAN topology is a hub and spoke. The hub location sits behind redundant NGFW appliances connected to multiple ISPs for Internet access. The spokes are P2P L2 circuits from the main router at the hub to each of the remote sites, eight in total. Spoke locations route all connectivity through the hub with the exception of Police who maintain their own CJIS and internet connections. They are also protected by dual NGFW appliances.

Q5) Please specify any hardware or software firewalls that will generate logs for the XDR solution. Include the make, model, and estimated daily throughput if possible.

A5) Firewalls are Fortigate 100Ds. They will be upgraded to the Fortigate 101F this summer. Do not have an estimated daily log at this time.

Q6) Are you able to estimate your expected event volume in either events per day or volume per day? If so, please specify

A6) We do not have an estimate of daily event volume.

Q7) Does your team include staff that will be able to understand alerts delivered by a managed Security Operations Center and ultimately remediate threats based on recommended actions?

A7) We have limited experience with threat remediation but have addressed a handful of incidents with the assistance of our current EDR vendor. Training with remediation tools and practices with respect to the vendor's security solution is part of our request.

Q8) To the best of your ability, please describe your expectations when it comes to automated response actions (SOAR).

A8) Our expectations are that SOAR actions will be able to provide our organization with the best opportunity to intervene when a threat is detected. We do not have a 24/7 SOC of our own and realize response time is crucial when dealing with both known and unknown threats. Our expectation is SOAR will allow us the ability to respond to a threat at multiple levels, endpoint, network, firewall and cloud to minimize and isolate threats.

Q9) What is the expected retention period(s) that are either written into your policies or generally accepted by your organization when it comes to the lifecycle of log, SIEM, or XDR data?

A9) We do not have a SIEM or XDR solution in place so we have no reference point but a minimum of 90 days would be expected with a consideration for up to a year.

Q10) Please advise the accurate number of seats to quote as Page 10 states "The City has a full time staff of four technology professionals supporting approximately ~280 users on ~290 endpoints." Page 19 states number of users "Require time for deployment across 5000 endpoints."

A10) That figure on Page 19 is incorrect. As a benchmark, please provide the metric for a deployment across 500 endpoints.

Q11) Is it possible to submit our proposal electronically?

A11) As stated in the RFP, physical copies of the RFP response are required.

Q12) Does the RFP require physical copies of the response to the RFP or will an emailed PDF suffice here?

A12) As stated in the RFP, physical copies of the RFP response are required.

Q13) Please advise if a deadline extension can be given as post office shipping can incur delays.

A13) The bid deadline will NOT be extended

Q14) How many endpoints do you currently have in your environment that need to be secured?

A14) We are budgeting for 290 endpoints. We would like the RFP responses to reflect the ability to increase the number of endpoints if necessary as our device count may fluctuate.

✗ xcitium

Company Address	US		Created Date	3/2/2023
Quote Number	00001001		Expiration Date	3/28/2023

Prepared By	Megan Tolmie		Contact Name	Gerald Crowley
Email	megan.tolmie@xcitium.com		Phone	(860) 489-2305
			Email	gerry_crowley@torringtonct.org

Bill To Name	City of Torrington		Ship To Name	City of Torrington
Bill To	140 Main St Torrington, Connecticut 6790 United States			

Product	Quantity	List Price	Term (Months)	Discount	Sales Price	Total Price
Professional Services for AEP (Cloud) - hourly rate	14.00	$250.00	12	20.00	$200.00	$2,800.00
Set-up fee for MDR - Small (up to 500)	1.00	$2,000.00	12	0.00	$2,000.00	$2,000.00
Xcitium Complete	290.00	$89.00	12	32.58	$60.00	$17,400.00

Product Amount	$17,400.00
PS Amount	$4,800.00
Grand Total	$22,200.00

✗ xcitium

XCITIUM COMPLETE

COMPREHENSIVE M(XDR) SECURITY

PROTECTING BUSINESS ECOSYSTEMS AT MACHINE SPEED WHILE CONNECTING
AND SECURING THE DOTS BETWEEN ENDPOINTS, CLOUDS & NETWORKS

WHAT IS XCITIUM COMPLETE?

Threat landscapes are ever-evolving. Defenders must stay several steps ahead of rapid-fire attackers while continuing to innnovate products, manage business operations, conquer the competition, accommodate remote workers, and provide security to endpoints, networks, and cloud infrastructures.

Meanwhile, ransomware attacks are on the rise, data breaches and IP theft is rampant and continuous, and defeated SOC teams industry wide are dealing with alert and staff fatigue at unprecedented levels. With massive increases in the volume and variety of attacks, everyone is asking whether today's detection-first cybersecurity approaches actually work. Who needs yet another M(XDR) detection product?

ENTERPRISES NEED XCITIUM COMPLETE M(XDR) BECAUSE WE NEVER TRUST, ALWAYS VERIFY

Xcitium's COMPLETE M(XDR) is an impotant paradigm shift. It is a uniquely differentiated MXDR service for endpoints, clouds, and networks that includes machine-speed ZeroDwell Containment across all the data points and vectors traversed by bad actors. MXDR extends across endpoints to continuously monitor, manage, and connect the dots across your entire technology stack. Our Kernel-level ZeroDwell virtualization is a pre-emptive prevention technology that precedes detection and response by containing Unknowns and potential attacks at runtime. This zero trust approach protects endpoints proactively while setting the groundwork for MXDR as a critical next step for offensively protecting, monitoring, securing, hardening and responding to known and unknown objects and future threats, including the deployment of advanced threat hunting at every level of your digital ecosystem − all from a single, unified platform. With automated containment as the innovative zero trust technology that distinguishes Xcitium from the glut of detection-first vendors in the marketplace, you receive only actionable alerts that accelerate the security team's ability to provide active responses via 24x7x365 managed SOC operations, because contained attacks are no longer threats.

KNOWN OR UNKNOWN THREATS, WE'VE GOT YOUR ENDPOINTS, CLOUDS & NETWORKS COVERED:

- STOP RANSOMS IN REAL TIME WITH ZERODWELL CONTAINMENT

- UNIFIED TECHNOLOGIES FOR ENDPOINTS, CLOUDS, & NETWORKS

- 24/7/365 EXPERT EYES ON GLASS & FULLY MANAGED SERVICES

- ADVANCED THREAT HUNTING & INTEGRATED GLOBAL INTEL

- CONTINUOUS MONITORING & PROACTIVE IOC DETECTION

- ANOMALOUS ENUMERATIONS & LATERAL MOVEMENT PREVENTION

- STEALTHY ATTACK CONTEXT & VISIBILITY: 40+ PROTOCOLS INCLUDING L7

- CROSS-STACK CORRELATION & HARDENING AGAINST FUTURE ATTACKS

- SCALE SECURITY TEAM WHILE ACCELERATING SOC EFFICIENCY (CONTAINED ATTACKS ARE NO LONGER THREATS SO ALL ALERTS ARE ACTIONABLE
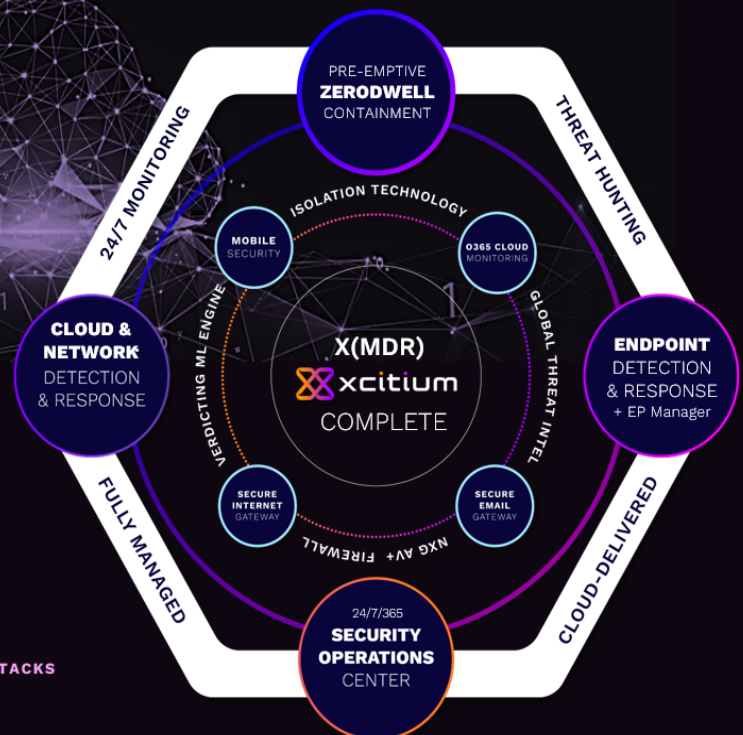
XCITIUM COMPLETE M(XDR) ADVANTAGES

XCITIUM COMPLETE M(XDR) is a comprehensive service that combines the capabilities of Xcitium's patented ZeroDwell Containment technology + all of the holistic, multi-layered capabilities of Xcitium Managed MDR + Xcitium M(XDR)'s advanced visibility, context, corrrelation, and **security ecosystem and data lake integration** woven together by automated AI and advanced machine learning capabilities. The key to any managed-XDR system is integraiton across an organization's security technology stack..

Xcitium MXDR's comprehensive integration and extensive visibility&context produces uniquely differentiated advantages:

- A siingle platform providing deep insight into stealth attacks that aid and accelerate the SOC team's abiility to step ahead of threat actors and harden against future attacks.

- Zero malware and ransomware dwell time, courtesy of Xcitium ZeroDwell Containment techology (this means contained attacks cannot dwell in, move laterally, or cause damage as a result of Xcitium's default virtualization of all unknowns at runtime).

- Rapid attack mitigation and vulnerability management, backed by advanced AI and ML with out-of-the-box security stack prevention and attack correlations. that lead to tremendously improved ROII for your business.

- Straightforward configuration, deploy,ment, and maintenance so you don't need additional staff to manage your security operations; we do all the heavy lifting for you.

M(XDR) INTEGRATIONS

GLOBAL THREAT INTL

ENDPOINTS

NETWORKS

CLOUDS

INTERNET | EMAIL GWs

APPLICATIONS

ZERO TRUST

M(XDR) SOLUTIONS

- 24/7/365 Eyes on Glass Alerting
- Weekly/Monthly Reporting
- Profile & Policy Management
- Pro-Active Threat Hunting & GLobal Threat Intel
- ZeroDwell Containment for Endpoints, Cloud & Network
- Human-Led Expert Incident Response / Forensics
- Live Remediation Support
- Monthly Security Meetings
- Security Ecosystem Integration
- Convergence of network security services & Zero Trust
- Network Monitoring:
  - NetworkLogTrafficVisibility (NTBA)
  - Intrusion Detection (IDS)
  - Additional Log Ingestion
  - Windows Event Logs
  - Firewall Logs
  - Linux Server Logs
  - Custom Data Sources
- Cloud Monitoring:
  - O365
  - Azure AD
  - AWS CloudTrail

M(XDR) USE CASES

IMMEDIATE TIME TO VALUE & REDUCED TCO

OPERATIONAL EASE WITH RICH, BUILT-IN INTEGRATIONS ACROSS THE ENTIRE SECURITY TECH STACK PROVIDING DEEP VISIBILITY, REAL TIME CONTEXT, AND AUTOMATED CONTAINMENT, DETECTION AND RESPONSE. ONLY ACTIONABLE ALERTS/ NO ALERT FATIGUE. FULLY INTEGRATED PLATFORM MEANS SIGNIFICANT REDUCTION IN TOTAL COST OF OWNERSHIP.

IR & PROACTIVE THREAT HUNTING

24/7/365 EYES ON GLASS ALERTING AND INCIDENT RESPONSE + FORENSIC ANALYSIS. PROACTIVE THREAT HUNTING QUERIES AND BUILT-IN SIEM FOR LOG INGESTION. PROFILE & POLICY MANAGEMENT AND LIVE REMEDIATION SUPPORT.

GLOBAL THREAT INTELLIGENCE

XCITIUM VERDICT CLOUD INTEGRATION WITH OPEN-SOURCE FEEDS THAT LEVERAGE INTERNAL INTELLIGENCE PLUS 300+ BEHAVIORAL ALERTS. DETAILED KILL-CHAIN REPORTS & EMERGING THREAT REPORTING WITH WEEKLY / MONTHLY SUMMARIES.

STREAMLINED EFFICIENCY

INCREASED SOC PRODUCTIVITY – ONE PLATFORM & ONE WORKFKLOW. AUTOMATED FORENSIC COLLECTION AND BLOCKING ACTIVITY IN REAL-TIME. ATTACK ISOLATION AT ENDPOINT, NETWORK & CLOUD WITH KERNEL-LEVEL API VIRTUALIZATION. ENDPOINT MANAGEMENT WITH REMOTE ACCESS. MOBILE DEVICE MANAGEMENT AND INTEGRATION.

ZERO BREACHES.   ZERO TRUST.   ZERO DOWNTIME.   ZERO DAMAGE.

WHY YOU NEED XCITIUM MXDR

01. Containment-Powered Protection: Security has never been a process of setting and forgetting. Now, attack intensity is increasing worldwide. It is more important than ever to protect first with ZeroDwell Containment, and then stay well ahead of attackers with managed detection, continuous monitoring, and expert attacker response strategies now that you are no longer burdened by alert fatigue.

02. Evolving Threat Landscape: Threats and attacks are continuously evolving and becoming more advanced, strategic and persistent. Ransomware attacks such as Nvidia and Toyota are just a few examples of notably-sized organizations that have suffered breaches. Without ZeroDwell Containment, organizations, regardless of size, are highly likely to experience a breach, and it is a matter of when, not if, it will happen.

03. Limited Person-Power: There are no shortcuts that can be taken to ensure an elevated level of dedicated security measures. You know your business and your customer better than anyone. Similarly, an MDR provider also knows its strengths in this line of business. With a lack of dedicated security expertise within your organization, partnering with an experienced XMDR provider is a must-have, not a nice to have.

04. Time and Cost: When deciding to develop and build an internal team for holistic security, or a committed team for incident response or threat hunting, the time and cost required can be prohibitive. By allowing you to focus on your business needs, Xcitium's dedicated XMDR solution allows you to focus your efforts entirely on analyzing events, conducting investigations, and observing round-the-clock monitoring.

05. Critical business value: With ZeroDwell protection coupled with a comprehensive, integrated XMDR solution that includes continuous monitoring and vulnerabilities guidance, organizations are able to conduct business at a level of comfort and security because their employees, IP, and infrastructure are managed expertly, and this posture helps to boost business productivity.

06. Enrich attack forensics with integrated threat intelligence: Xcitium Complete integrates threat intelligence with containment, telemetry, and proprietary detection sources to empower security teams with context-rich data and Indicators of Compromise (Ioc), including IP addresses, hashes, revealed vulnerabilities, and at-risk domains. This accelerates proactive forensics and triage capabilities.

BUSINESS REWARDS

• Proactive protection for endpoints, networks and clouds using Xcitium's ZeroDwell Containment automated virtualization technology to isolate all unknowns and reduce the attack surface.

• Real-time monitoring, alerting, aggregating and reporting of suspicious activity and telemetry sensor data for endpoints, networks, and clouds.. Gain real time automated ML and AI-built context and correlations.

• Security event alert management

• Endpoint management

• Incident response management and investigation to proactively reveal advanced attacks and stealth strategies.

• Dedicated Xcitium SOC IR expert analysts for accelerated analysis, forensics, and hardening against future threats.

• Managed proactive threat hunting capabilities to expose and pinpoint threats and attacker profiles.

• Advanced analytics highlighting file, user, application, and endpoint data.

• 24 x 7 SOC support through numerous geographical centers

ABOUT US

Xcitium, formerly known as Comodo Security Solutions, is used by more than 3,000 organizational customers & partners around the globe. Xcitium was founded with one simple goal — to put an end to cyber breaches. Our patented ZeroDwell technology uses Kernel-levle API Virtualization to isolate and remove threats like zero-day malware & ransomware before they cause any damage to any endpoints. ZeroDwell is the cornerstone of Xcitium's endpoint suite which includes pre-emptive endpoint containment, endpoint detection & response (EDR), and managed detection & response (MDR). Since inception, Xcitium has a track record of zero breaches when fully configured.

CONTACT

sales@xcitium.com • support@xcitium.com

2022 EDITION - SOLUTION BRIEF

Implementation Consulting Services

xcitium

What We Do

All Xcitium implementation consulting services start with a kick-off and design session. Projects must align with customer corporate goals and security requirements that drove the software acquisition. We adapt our proven templates, your team gains the necessary experience to sustain a successful implementation.

The Xcitium consulting approach follows a proven flexible methodology. The key to success is designing an implementation to fit your infrastructure, staff availability, staff and experience, operational practices and corporate goals.

Our approach is simple: understand requirements, test and expand. We iterate through your various work groups and profiles based on this fundamental approach.

Plan, Execute, Manage

01
- Requirements
- Plan
- Risks
- Expectations
- Budget

Consulting, Me Consulting, Mentoring,

Pilot Implementation

02
- Cross Functional
- Validate
- Operationalize
- Integrate

Consulting, Me Consulting, Mentoring,

Enterprise Rollout

03
- Release Management
- Continual Assessment
- Constant Tuning
- Expanded Operations

Consulting, Me Consulting, Mentoring,

Ongoing Operations

04
- Administration
- Tuning
- Monitoring
- Sustainingut

Customer Care

At A Glance

- ✓ Integrate with existing security policies and processes
- ✓ Operational results
- ✓ Adapt proven methods
- ✓ Create self-sustaining experience and expertise
- ✓ Guide and mentor towards successful end-to-end implementation

Why Our Services

- ✓ Proven IT and security expertise
- ✓ Adapt proven methods
- ✓ Experienced consultants, mentors, and instructors
- ✓ Administrative background
- ✓ Projects managed for success

What We Provide

- ✓ Guided Implementations
- ✓ Advanced Implementations
- ✓ As-Needed Consulting
- ✓ Health Checks
- ✓ Ongoing Technical Services

Guided Implementations

Your experienced team benefits from our programmatic approach to implementing security solutions. Xcitium provides project management and consulting to ensure that the implementation meets customer needs in a timely and efficient manner. Your staff will learn from our training programs and our consultative approach to assure uneventful ongoing operations and administration of your Xcitium
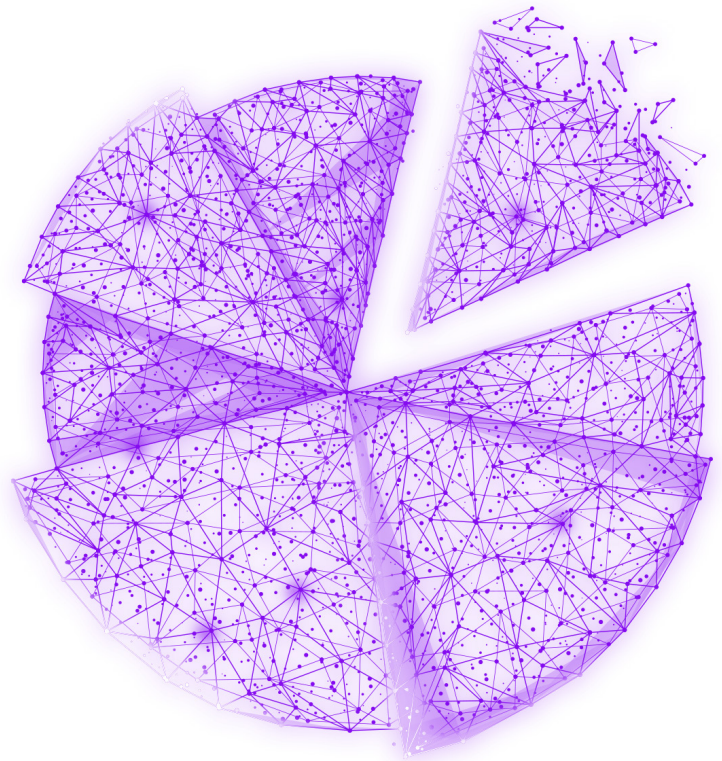
implementation.

Advanced Implementation

Xcitium works with your team to provide project management and experienced consultants to deliver custom implementation plans and tasks. Sample projects include: deploying to new OS platforms, third party replacements, assessing operations, integrating Xcitium's best practices into your operations, providing specific tuning and configuration for complex environments. Our goal: efficient and timely completion of our consulting projects in your complex and dynamic enterprise.

As Needed Consulting

Our experienced consultants support your efforts to implement and adopt Xcitium products to meet your overall security goals. Your team can leverage our training and proven methodology to streamline the implementation. Our consultants will verify your implementation strategy and processes, help design the most viable approach, and provide ongoing feedback to ensure you are gaining real world value from Xcitium products and consulting services.

Health Checks

Cybersecurity is an ongoing process. Organizations, applications, infrastructure, operations – they're always changing. The Xcitium Health Check ensures you are following industry best practices and taking advantage of the latest product features and functions. The Xcitium Health Check includes assessing performance and suggesting ongoing updates and adjustments to sustain your implementation

ABOUT US

Xcitium, formerly known as Comodo Security Solutions, is used by more than 3,000 organizational customers & partners around the globe. Founded with one simple goal – to put an end to cyber breaches. Xcitium's patented 'ZeroDwell' technology uses Kernel API Virtualization to isolate and remove threats like zero-day malware & ransomware before they cause any damage. ZeroDwell is the cornerstone of Xcitium's endpoint suite which includes ZeroDwell Containment, endpoint detection & response (EDR), managed detection & response (MDR) and managed XDR (M[X]DR). Since inception, Xcitium has a zero breach track record when fully configured.

CONTACT

1800-GET-XCITIUM • sales@xcitium.com • support@xcitium.com

Xcitium ZeroDwell Warranty Program

Xcitium ZeroDwell Warranty Addendum

This Xcitium ZeroDwell Warranty Addendum ("**Warranty**") describes the terms and conditions for the provision of the ZeroDwell Warranty provided from Xcitium Inc. ("**Xcitium**") to either the Xcitium customer pursuant to the Xcitium License Agreement or to the managed security service provider (MSP) pursuant to the MSP Agreement (each a "**Company**") who subscribes to its Xcitium Advanced, Xcitium Managed MDR or Xcitium Complete M(X)DR services on Xcitium's Platform or Xcitium Enterprise Platform ("**Xcitium Platform**", respectfully) under the Xcitium License Agreement. These Warranty terms govern the Warranty, provided that such Warranty is stated in a signed Quote or Purchase Order among Xcitium and the Company, or an approved Xcitium Partner and the Company, in each case, where approved by Xcitium (collectively, "**PO**"). This Warranty shall be effective as of the date the PO is executed ("**Effective Date**") and shall remain in effect for the term of the Warranty stated in such PO and so long as the Company subscribes to the Xcitium Advanced, Xcitium Managed MDR or Xcitium Complete M(X)DR service in accordance with the License Agreement and uses the Xcitium Advanced, Xcitium Managed MDR or Xcitium Complete M(X)DR service in compliance with the terms of this Warranty Agreement (including, without limitation, the Xcitium Advanced, Xcitium Managed MDR or Xcitium Complete M(X)DR service configuration ("**Warranty Term**"). As the Company's authorized representative, you represent that you are authorized by the Company to accept the Warranty as part of the Company's subscription to the Xcitium Advanced, Xcitium Managed MDR or Xcitium Complete M(X)DR service. Capitalized terms shall have the meaning assigned to such terms where defined in this Warranty, and capital terms used but not defined in this Warranty shall have the meaning assigned to such terms in the License Agreement.

Subject to the terms and conditions described herein and the License Agreement, Xcitium states as follows:

SPECIFIC ZERODWELL WARRANTY

1. **Warranty**. During the Warranty Term, so long as the Company also subscribes to the Xcitium Advanced, Xcitium Managed MDR or Xcitium Complete M(X)DR service in compliance with the License Agreement, the Company's Endpoints will be protected by the Xcitium Advanced, Xcitium Managed MDR or Xcitium Complete M(X)DR service to prevent a successful Ransomware attack. The Warranty granted herein shall apply to all such Endpoints provided that:

    a)   The Xcitium Advanced, Xcitium Managed MDR or Xcitium Complete M(X)DR service and Endpoints are deployed in accordance with the Xcitium recommendations, and such Endpoints are currently active and properly configured;

    b)   Only Files that are on Endpoints with current, licensed Xcitium Advanced agent or covered under Xcitium Managed MDR or Xcitium Complete M(X)DR services are covered under this Warranty;

c)   The Xcitium Advanced or Xcitium Managed MDR or Xcitium Complete M(X)DR service and all Endpoints of the Company have the following required configurations and attributes:

1. Xcitium Advanced, Xcitium Managed MDR or Xcitium Complete M(X)DR service active and properly licensed;

2. ZeroDwell agent:

•   Xcitium Client Communications (XCC) and Xcitium Client Security (XCS) agents are updated to latest n-1 version on compatible endpoints as indicated in Xcitium technical specifications.

•   Anti-virus database is current and updated regularly per Xcitium policy. There are no efforts by the Customer to block updates in Customer environment, e.g. ports are blocked by a firewall, Cloud Connectivity is disabled, etc.

•   Client Access control is protected by a secure password and does not allow local override of profiles.

•   Two-factor authentication from Xcitium portal is enabled without addition of any generic Admin User implemented via a generic email address (multi-user).

3. Configuration and Change Restrictions:

•   Rules under the configuration setting sections are not disabled or modified for protection layers such as, but not limited to, Containment, HIPS, Miscellaneous and Firewall layers.

•   Learning/training mode in profile on non-gold-images or directly on production machines not enabled.

•   The order of default rules created during the initial deployment process have not been changed or altered.

•   Exclusions specified by Xcitium are not deployed in the Xcitium Platform or Endpoints.

•   There are no items added to shared spaces that ultimately lead to an infection.

•   There are no User(s) with admin access running a customized script/procedure that ultimately lead to an infection.

•   Customer exclusions (file paths / file names) are not implemented that lead to an infection.

•   Malware incorrectly categorized as 'Trusted' by Customer is not covered under warranty.

4. Operating system:

•   The Warranty applies to Standard Windows Agents, and on supported versions of Microsoft Windows (as specified by Xcitium).

- Each Endpoint is malware-free prior to Xcitium Agent installation.

- OS is fully updated and patched for security updates on each covered Endpoint, and all vulnerable applications are updated to latest releases.

5. Platform:

- A supported version of the Xcitium Platform and agent(s) are deployed.

d. The Company notifies Xcitium of the Ransomware discovery within 12 hours at warranty@Xcitium.com and adheres to instructions provided by appropriate Xcitium services personnel and provides any and all requested information to Xcitium.

2. **Scope of the Warranty.** Subject to the terms of this Warranty , including the specific requirements of Section 1 above, in case of a successful ransomware attack on Endpoints covered by the Warranty, as shown and established in Xcitium's logs and other records, Xcitium will make a single refund payment in an amount equivalent to the actual license fee payments which were made to Xcitium equal to the lesser of either: a.) the monthly payments to Xcitium for the current contract or b.) the most recent twelve (12) months payments. In no event shall the total amount refunded under a.) or b.) exceed a maximum of One Million U.S. Dollars ($1,000,000). For clarity, this Warranty applies only to environments in which Endpoints with Xcitium ZeroDwell Agent are installed and configured as described above.

3. **Condition Precedent to Warranty Payment**. Xcitium shall only provide the remedy for the Breach of the Warranty as described above if: (i) the Ransomware attack has occurred, is discovered by the Company and reported to Xcitium during the Warranty Term and Company's subscription to the Xcitium Advanced, Xcitium Managed MDR or Xcitium Complete M(X)DR service under the License Agreement; (ii) sufficient evidence that Company's Endpoints and the Xcitium Advanced, Xcitium Managed MDR or Xcitium Complete M(X)DR service were properly configured and fully compliant with Section 1 above when the Ransomware attack occurred; (iii) the Company demands in writing to recover license fees paid per Section 1 above; and (iv) sufficient evidence and written assurances are provided by the Company that no Warranty payment would be used by the Company to make a payment to any person or entity subject to economic sanctions administered or enforced by the U.S. Treasury Department Office of Foreign Assets Control (OFAC), including any such person or entity listed on OFAC's the Specially Designated Nationals and Blocked Persons (SDN) list or otherwise prohibited under relevant U.S. law; and (v) Company provides Xcitium with all requested assistance and information in order to investigate the Ransomware attack.

4. **Exclusions**: The Warranty shall not apply to a breach caused primarily by (i) any deployment, configuration and/or use of the Xcitium Advanced, Xcitium Managed MDR or Xcitium Complete M(X)DR service (or a portion thereof), for any or no reason, in a manner inconsistent with the requirements of Section 1 herein; (ii) Company's negligence or misconduct; or (iii) other products and/or services which directly or indirectly cause the malfunction or non-performance of the Xcitium Advanced, Xcitium Managed MDR or Xcitium

Complete M(X)DR service with respect to the subject Ransomware; or (iv) an endpoint is infected that does not have Xcitium Advanced fully installed or Xcitium Managed MDR or Xcitium Complete M(X)DR service fully operational; or (v) the infected endpoint or device occurred prior to full deployment of Xcitium Advanced, Xcitium Managed MDR or Xcitium Complete M(X)DR service was fully operational; (vi) the infection has been classified as a "Potentially Unwanted Program" or "Potentially Unwanted Application"; or (vii) any pre-existing condition on the network or endpoint device prior to the Effective Date .

5. **Sole and Exclusive Remedy**. The aforementioned remedy for the Breach shall be the Company's sole and exclusive remedy and the entire liability of Xcitium for any Breach of the Warranty.

6. **Definitions**. The capitalized terms below shall have the following meaning:

   a. "**Breach**" or "**Security Incident**" or "**Ransomware Breach**" means the unauthorized access to at least one Xcitium Protected Endpoint in the form of Ransomware which has caused material harm to the Company. "Material harm" must include: (1) a malicious actor outside of the company or company affiliates acquiring, without authorization, unencrypted digital data that compromises the security, confidentiality, or integrity of personal information or confidential information maintained by the Company, (2) public disclosure or threat of public exposure of such personal information or confidential information, and (3) the compromise of at least one Company Endpoint resulting in the blocking of access of data or information on such Endpoint.

   b. "**License Agreement**" shall mean either the End-User License Agreement or the MSP Agreement as applicable to the Company.

   c. "**Ransomware**" means a malware software program that infects Company's systems from external sources (i.e., in the wild), which installs, persists and encrypts at least a large majority of files at the operating system level, and continuing to demand payment (the "Ransom") in order to decrypt the encrypted files. For clarification, Ransomware does not include any malware introduced by the Company or any third party to Company's internal systems, whether intentionally (i.e., malware testing) or through a breach or unauthorized access in the system's security.

   d. "**Endpoints**" means physical or virtual computing devices that can process data.

7. Other Terms and Conditions. Any other terms and conditions of the License Agreement shall be unaffected by this Warranty, except as expressly stated in the License Agreement. In case of any conflict between the terms of this Warranty and the terms and conditions within the License Agreement relating to the Warranty, the terms and conditions within this Warranty shall prevail.

8. Miscellaneous. This Warranty represents the complete understanding between the Parties concerning the Warranty granted hereunder and supersedes any and all prior agreements or representations between the Parties. Xcitium may revise the terms of this Warranty from time to time in its reasonable discretion by providing written notice, provided that such revisions shall not reduce or eliminate the monetary remedy described in Section 2 herein.

To the extent that Xcitium pays to the Company under the Warranty, Company agrees that Xcitium shall acquire a subrogation right to assert a claim against the actor(s) who delivered the Ransomware to Company and caused damages for which Xcitium incurred Warranty costs, and Company further agrees to assist Xcitium should it decide to assert a claim against such actor. If any provision of this Warranty is held to be unenforceable for any reason, such provision shall be reformed only to the extent necessary to make it enforceable. This Warranty is governed by and construed in accordance with the substantive laws of the State of New Jersey, irrespective of its choice of law principles, and the competent courts in the State of New Jersey shall have sole and exclusive jurisdiction over every dispute arising from, or in connection with this Warranty.

ABOUT US

Xcitium, formerly known as Comodo Security Solutions, is used by more than 3,000 organizational customers & partners around the globe. Founded with one simple goal – to put an end to cyber breaches. Xcitium's patented 'ZeroDwell' technology uses Kernel API Virtualization to isolate and remove threats like zero-day malware & ransomware before they cause any damage. ZeroDwell is the cornerstone of Xcitium's endpoint suite which includes ZeroDwell Containment, endpoint detection & response (EDR), managed detection & response (MDR) and managed XDR (M[X]DR). Since inception, Xcitium has a zero breach track record when fully configured.

CONTACT

1800-GET-XCITIUM • sales@xcitium.com • support@xcitium.com