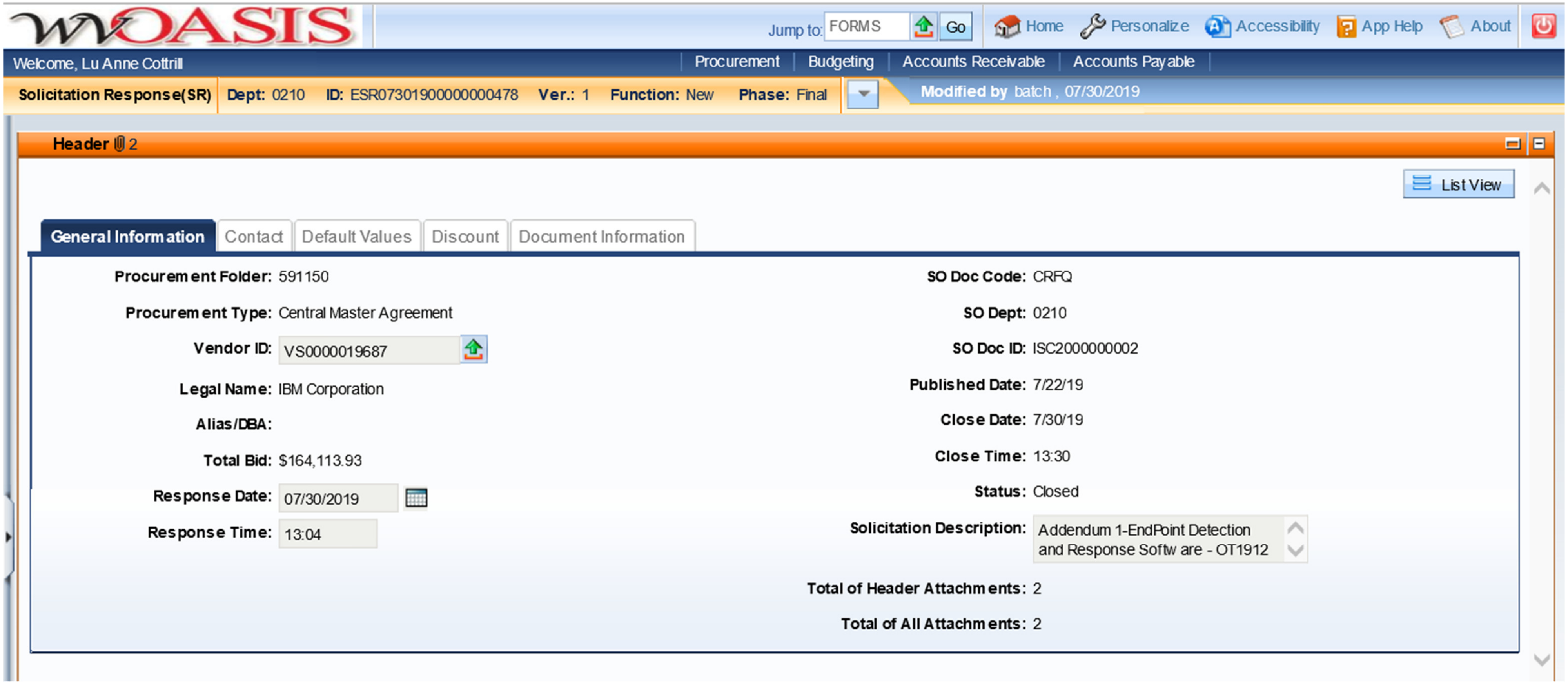
West Virginia
Purchasing Division

2019 Washington Street, East
Charleston, WV 25305
Telephone: 304-558-2306
General Fax: 304-558-6026
Bid Fax: 304-558-3970



Welcome, Lu Anne Cottrill

Solicitation Response(SR) **Dept:** 0210 **ID:** ESR073019000000000478 **Ver.:** 1 **Function:** New **Phase:** Final

Modified by batch , 07/30/2019

Header 2

Procurement Folder:	591150	**SO Doc Code:**	CRFQ
Procurement Type:	Central Master Agreement	**SO Dept:**	0210
Vendor ID:	VS0000019687	**SO Doc ID:**	ISC2000000002
Legal Name:	IBM Corporation	**Published Date:**	7/22/19
Alias/DBA:		**Close Date:**	7/30/19
Total Bid:	$164,113.93	**Close Time:**	13:30
Response Date:	07/30/2019	**Status:**	Closed
Response Time:	13:04	**Solicitation Description:**	Addendum 1-EndPoint Detection and Response Softw are - OT1912
		Total of Header Attachments:	2
		Total of All Attachments:	2

Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder : 591150

Solicitation Description : Addendum 1-EndPoint Detection and Response Software - OT1912

Proc Type : Central Master Agreement

Date issued	Solicitation Closes	Solicitation Response	Version
	2019-07-30 13:30:00	SR 0210 ESR07301900000000478	1

VENDOR

VS0000019687

IBM Corporation

Solicitation Number: CRFQ 0210 ISC2000000002

Total Bid : $164,113.93 **Response Date:** 2019-07-30 **Response Time:** 13:04:48

Comments:

FOR INFORMATION CONTACT THE BUYER

Jessica S Chambers
(304) 558-0246
jessica.s.chambers@wv.gov

Signature on File **FEIN #** **DATE**

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	Overall Total for Contract Items 1 & 2 with Opt Renewals	1.00000	LS	$164,113.930000	$164,113.93

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item 1: Containment & Remediation

4.1.1.1 The Vendor must provide a software and/or service that is capable of supporting a minimum of 2,000 endpoints throughout the State of West Virginia

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, **WV** 25305-0130

State of West Virginia
Request for Quotation
21 - Info Technology

Proc Folder: 591150

Doc Description : EndPoint Detection and Response Software - OT19125

Proc Type: Central Master Aareement

Date Issued	Solicitation Closes	Solicitation No	Version
2019-07-10	2019-07-30 13:30:00	CRFQ 0210 ISC2000000002	1

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON STE
CHARLESTON WV 25305
US

VENDOR

Vendor Name, Address and Telephone Number:

IBM Corportation,
1 New Orchard Rd
Armonk, NY 10504
United States,
321-505-3066

FOR **INFORMATION** CONTACT THE BUYER

Jessica S Chambers
(304) 558-0246
jessica.s.chambers@wv.gov

Signature X FEIN# DATE

All offers subjectto all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION:

The West Virginia Purchasing Division is soliciting bids on behalf of The WV Office of Technology to establish a contract for an End Point Detection and Response Software to support approximately two thousand (2,000) endpoints across the state of West Virginia but can be managed centrally. This service will assist in the continuous monitoring and response to advanced cyber security threats per the terms and conditions and specifications as attached.

INVOICE TO	SHIP TO
 DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV25305 US	IS&C - CHIEF FINANCIAL OFFICER DEPARTMENT OF ADMINISTRATION BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON **WV** 25305 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
	Overall Total for Contract Items 1 & 2 with Opt Renewals	1.00000	LS		

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item 1: Containment & Remediation

4.1.1.1 The Vendor must provide a software and/or service that is capable of supporting a minimum of 2,000 endpoints throughout the State of West Virginia

For more details see attached specifications.

INSTRUCTIONS TO VENDORS SUBMITTING BIDS

1. REVIEW DOCUMENTS THOROUGHLY: The attached documents contain a solicitation for bids. Please read these instructions and all documents attached in their entirety. These instructions provide critical information about requirements that if overlooked could lead to disqualificationof a Vendor's bid. All bids must be submitted in accordance with the provisions contained in these instructions and the Solicitation. Failure to do so may result in disqualification of Vendor's bid.

2. MANDATORY TERMS: The Solicitation may contain mandatory provisions identified by the use of the words "must," **"will,"** and "sha ll." Failure to comply with a mandatory term in the Solicitation will result in bid disqualification.

3. PREBID MEETING: The item identified below shall apply to this Solicitation.

0 A pre-bid meeting will not be held prior to bid opening

□ A **MANDATORY PRE-BID** meeting will be held at the following place and time:

All Vendors submitting a bid must attend the mandatory pre-bid meeting. Failure to attend the mandatory pre-bid meeting shall result in disqualification of the Vendor's bid. No one person attending the pre-bid meeting may represent more than one Vendor.

An attendance sheet provided at the pre-bid meeting shall serve as the official document verifying attendance . The State will not accept any other form of proof or documentation to verify attendance. Any person attending the pre-bid meeting on behalf of a Vendor must list on the attendance sheet his or her name and the name of the Vendor he or she is representing.

Additionally, the person attending the pre-bid meeting should include the Vendor' s E-Mail address, phone number, and Fax number on the attendance sheet. It is the Vendor's responsibility to locate the attendance sheet and provide the required information. Failure to complete the attendance sheet as required may result in disqualificationof Vendor's bid.

All Vendors should arrive prior to the starting time for the pre-bid. Vendors who arrive after the starting time but prior to the end of the pre-bid will be permitted to sign in, but are charged with knowing all matters discussed at the pre-bid.

Questions submitted at least five business days prior to a scheduled pre-bid will be discussed at the pre-bid meeting if possible. Any discussions or answers to questions at the pre-bid meeting are preliminary in nature and are non-binding.Official and binding answers to questions will be published in a written addendum to the Solicitation prior to bid opening.

4. VENDOR QUESTION DEADLINE: Vendors may submit questions relating to this Solicitation to the Purchasing Division. Questions must be submitted in writing. All questions must be submitted on or before the date listed below and to the address listed below in order to be considered. A written response will be published in a Solicitation addendum if a response is possible and appropriate. Non-written discussions, conversations, or questions and answers regarding this Solicitation are preliminary in nature and are nonbinding.

Submitted e-mails should have solicitation number in the subject line.

Question Submission Deadline: July 18 , 2019 at 9:00 **AM (EDT)**

Submit Questions to: Jessica
Chambers 2019 Washington
Street, East Charleston, WV 25305
Fax: (304) 558-4115 (Vendors should not use this fax number for bid submission)
Email: Jessica.S.Chambers@wv.gov

5. VERBAL COMMUNICATION: Any verbal communication between the Vendor and any State personnel is not binding, including verbal communication at the mandatory pre-bid conference. Only information issued in writing and added to the Solicitation by an official written addendum by the Purchasing Division is binding.

6. BID SUBMISSION: All bids must be submitted electronically through wvOASIS or signed and delivered by the Vendor to the Purchasing Division at the address listed below on or before the date and time of the bid opening. Any bid received by the Purchasing Division staff is considered to be in the possession of the Purchasing Division and will not be returned for any reason. The Purchasing Division will not accept bids, modification of bids, or addendum acknowledgment forms via e-mail. Acceptable delivery methods include electronic submission via wvOASIS, hand delivery, delivery by courier, or facsimile.

The bid delivery address is:
Department of Administration, Purchasing
Division 2019 Washington Street East
Charleston, WV 25305-0130

A bid that is not submitted electronically through wvOASIS should contain the information listed below on the face of the envelope or the bid may be rejected by the Purchasing Division.:

SEALED BID:

BUYER: Jessica Chambers
SOLICITATION NO.: CRFQ ISC2000000002
BID OPENING DATE:
7/30/2019 BID OPENING
TIME: 1:30 PM (EDT) FAX
NUMBER: (304)558-3970

The Purchasing Division may prohibit the submission of bids electronically through wvOASIS at its sole discretion. Such a prohibition will be contained and communicated in the wvOASIS system resulting in the Vendor's inability to submit bids through wvOASIS. Submission of a response to an Expression or Interest or Request for Proposal is not permitted in wvOASIS.

For Request For Proposal ("RFP") Responses Only: In the event that Vendor is responding to a request for proposal, the Vendor shall submit one original technical and one original cost proposal plus____convenience copies of each to the Purchasing Division at the address shown above. Additionally, the Vendor should identify the bid type as either a technical or cost proposal on the face of each bid envelope submitted in response to a request for proposal as follows:

BID TYPE: (This only applies to CRFP)
D Technical
D Cost

7. BID OPENING: Bids submitted in response to this Solicitation will be opened at the location identified below on the date and time listed below. Delivery of a bid after the bid opening date and time will result in bid disqualification. For purposes of this Solicitation, a bid is considered delivered when confirmation of delivery is provided by wvOASIS (in the case of electronic submission) or when the bid is time stamped by the official Purchasing Division time clock (in the case of hand delivery).

Bid Opening Date and Time: July 30 2019 at 1:30 **PM (EDT)**

Bid Opening Location: Department of Administration, Purchasing
Division 2019 Washington Street East
Charleston, WV 25305-0130

8. ADDENDUM ACKNOWLEDGEMENT: Changes or revisions to this Solicitation will be made by an official written addendum issued by the Purchasing Division. Vendor should acknowledge receipt of all addenda issued with this Solicitation by completing an Addendum Acknowledgment Form, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification.The addendum acknowledgementshould be submitted with the bid to expedite document processing.

9. BID FORMATTING: Vendor should type or electronically enter the information onto its bid to prevent errors in the evaluation. Failure to type or electronically enter the information may result in bid disqualification.

10. ALTERNATE MODEL OR BRAND: Unless the box below is checked, any model, brand, or specification listed in this Solicitation establishes the acceptable level of quality only and is not intended to reflect a preference for, or in any way favor, a particular brand or vendor. Vendors may bid alternates to a listed model or brand provided that the alternate is at least equal to the model or brand and complies with the required specifications.The equality of any alternate being bid shall be determined by the State at its sole discretion. Any Vendor bidding an alternate model or brand should clearly identify the alternate items in its bid and should include manufacturer's specifications, industry literature, and/or any other relevant documentation demonstrating the

equality of the alternate items. Failure to provide information for alternate items may be grounds for rejection of a Vendor' s bid.

D This Solicitation is based upon a standardized commodity established under W. Va. Code§ SA-3-61. Vendors are expected to bid the standardized commodity identified. Failure to bid the standardi zed commodity will result in your firm's bid being rejected.

11. EXCEPTIONS AND CLARIFICATIONS: The Solicitation contains the specifications that shall form the basis of a contractual agreement. Vendor shall clearly mark any exceptions, clarifications, or other proposed modifications in its bid. Exceptions to, clarifications of, or modifications of a requirement or term and condition of the Solicitation may result in bid disqualification.

12. COMMUNICATION LIMITATIONS: In accordancewith West Virginia Code of State Rules §148-1-6.6, communication with the State of West Virginia or any of its employees regarding this Solicitation during the solicitation, bid, evaluation or award periods, except through the Purchasing Division, is strictly prohibited without prior Purchasing Division approval. Purchasing Division approval for such communication is implied for all agency delegated and exempt purchases.

13. REGISTRATION: Prior to Contractaward, the apparent successful Vendor must be properly registered with the West Virginia Purchasing Division and must have paid the $125 fee, if applicable.

14. UNIT PRICE: Unit prices shall prevail in cases of a discrepancy in the Vendor' s bid.

15. PREFERENCE: Vendor Preference may be requested in purchases of motor vehicles or construction and maintenance equipment and machinery used in highway and other infrastructure projects. Any request for preference must be submitted in writing with the bid, must specifically identify the preference requested with reference to the applicable subsection of West Virginia Code§ SA-3-37, and should include with the bid any info rmat ion necessary to evaluate and confirm the applicability of the requested preference. A request form to help facilitate the request can be found at: http://www.state.wv.us/ admin/purchase/vrc/Venpref.pdf.

15A. RECIPROCAL PREFERENCE: The State of West Virginia applies a reciprocal preference to all solicitations for commodities and printing in accordance with W. Va. Code§ 5A-3-37(b). In effect, non-resident vendors receiving a preference in their home states, will see that same preference granted to West Virginia resident vendors bidding against them in West Virginia. A request form to help facilitate the request can be found at: http://www.state.wv.us/admin/purchase/vrcN enpref.pdf.

16. SMALL, WOMEN-OWNED, OR MINORITY-OWNEDBUSINESSES: For any solicitationspublicl y advertised for bid, in accordance with West Virginia Code §5A-3- 37(a)(7) and W. Va. CSR§ 148-22-9, any non-resident vendor certified as a sma ll, women- owned, or minority-owned business under W. Va. CSR § 148-22-9 shall be providedthe same preference made available to any resident vendor. Any non-resident small, women-owned, or minority-owned business must identify itself as such in writing, must submit that writing to the

Purchasing Division with its bid, and must be properly certified under W. Va. CSR§ 148-22-9 prior to contract award to receive the preferences made available to resident vendors. Preference for a non-resident small, women-owned, or minority owned business shall be applied in accordance with W. Va. CSR§ 148-22-9.

17. WAIVER OF MINOR IRREGULARITIES: The Director reserves the right to waive minor irregularities in bids or specifications in accordance with West Virginia Code of State Rules§ 148-1-4.6.

18. ELECTRONIC FILE ACCESS RESTRICTIONS: Vendor must ensure that its submission in wvOASIS can be accessed and viewed by the Purchasing Division staff immediately upon bid opening. The Purchasing Division will consider any file that cannot be immediately accessed and viewed at the time of the bid opening (such as, encrypted files, password protected files, or incompatible files) to be blank or incomplete as context requires, and are therefore unacceptable. A vendor will not be permitted to unencrypt files, remove password protections, or resubmit documents after bid opening to make a file viewable if those documents are required with the bid. A Vendor may be required to provide document passwords or remove access restrictions to allow the Purchasing Division to print or electronically save documents provided that those documents are viewable by the Purchasing Division prior to obtaining the password or removing the access restriction.

19. NON-RESPONSIBLE: The Purchasing Division Director reserves the right to reject the bid of any vendor as Non-Responsible in accordance with W. Va. Code of State Rules § 148-1- 5.3, when the Director determines that the vendor submitting the bid does not have the capability to fully perfonn, or lacks the integrity and reliability to assure good-faith performance."

20. ACCEPTANCE/REJECTION: The State may accept or reject any bid in whole, or in part in accordance with W. Va. Code of State Rules§ 148-1-4.5. and § 148-1-6.4.b."

21. YOUR SUBMISSION IS A PUBLIC DOCUMENT: Vendor' s entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code§§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom oflnforrnation Act West Virginia Code §§ 29B-1-1 et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," " proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.

22. INTERESTED PARTY DISCLOSURE: West Virginia Code§ 6D-1-2 requires that the vendor submit to the Purchasing Division a disclosure of interested parties to the contract for all contracts with an actual or estimated value of at least $1 Million. That disclosure must occur on the form prescribed and approved by the WV Ethics Commission prior to contract award. A copy of that form is included with this solicitation or can be obtained from the WV Ethics Commission. This requirement does not apply to publicly traded companies listed on a national or international stock exchange. A more detailed definition of interested parties can be obtained from the form referenced above.

23. WITH THE BID REQUIREMENTS: In instances where these specifications require documentation or other information with the bid, and a vendor fails to provide it with the bid, the Director of the Purchasing Division reserves the right to request those items after bid opening and prior to contract award pursuant to the authority to waive minor irregularities in bids or specifications under W. Va. CSR§ 148-1-4.6. This authority does not apply to instances where state law mandates receipt with the bid.

GENERAL TERMS AND CONDITIONS:

1. CONTRACTUAL AGREEMENT: Issuanceof a Award Document signed by the Purchasing Division Director, or his designee, and approved as to form by the Attorney General's office constitutes acceptance of this Contract made by and between the State of West Virginia and the Vendor. Vendor's signature on its bid signifies Vendor's agreement to be bound by and accept the terms and conditions contained in this Contract.

2. DEFINITIONS: As used in this Solicitation/Contract, the following terms shall have the meanings attributed to them below. Additional definitions may be found in the specifications included with this Solicitation/Contract.

2.1. "Agency" or "Agencies" means the agency, board, commission, or other entity of the State of West Virginia that is identified on the first page of the Solicitation or any other public entity seeking to procure goods or services under this Contract.

2.2. "Bid" or "Proposal" means the vendors submitted response to this solicitation.

2.3. "Contract" means the binding agreement that is entered into between the State and the Vendor to provide the goods or services requested in the Solicitation.

2.4. "Director" means the Director of the West Virginia Department of Administration, Purchasing Division.

2.5. "Purchasing Division" means the West Virginia Department of Administration, Purchasing Division.

2.6. "Award Document" means the document signed by the Agency and the Purchasing Division, and approved as to form by the Attorney General, that identifies the Vendor as the contract holder.

2.7. "Solicitation"means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

2.8. "State" means the State of West Virginia and/or any of its agencies, commissions, boards, etc. as context requires.

2.9. "Vendor" or "Vendors" means any entity submitting a bid in response to the Solicitation, the entity that has been selected as the lowest responsible bidder, or the entity that has been awarded the Contract as context requires.

3. CONTRACT TERM; RENEWAL; EXTENSION: The term of this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below:

0 **Term Contract**

Initial Contract Term: Initial Contract Term: This Contract becomes effective on upon award and extends for a period of one (1) year(s).

Renewal Term: This Contract may be renewed upon the mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any request for renewal should be delivered to the Agency and then submitted to the Purchasing Division thirty (30) days prior to the expiration date of the initial contract term or appropriate renewal term. A Contract renewal shall be in accordance with the terms and conditions of the original contract. Unless otherwise specified below, renewal of this Contract is limited to three(3) successive one (1) year periods or multiple renewal periods of less than one year, provided that the multiple renewal periods do not exceed the total number of months available in all renewal years combined.

Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

D **Alternate Renewal Term** - This contract may be renewed for__________________ successive __________ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

Delivery Order Limitations: 1n the event that this contract permits delivery orders, a delivery order may only be issued during the time this Contract is in effect. Any delivery order issued within one year of the expiration of this Contract shall be effective for one year from the date the delivery order is issued. No delivery order may be extended beyond one year after this Contract has expired.

D **Fixed Period Contract:** This Contract becomes effective upon Vendor' s receipt of the notice to proceed and must be completed within _ _ _ _ _ _ _ _ _ _ _ days.

D **Fixed Period Contract with Renewals:** This Contract becomes effective upon Vendor' s receipt of the notice to proceed and part of the Contract more fully described in the attached specifications must be completed within ________________ days. Upon completion of the work covered by the preceding sentence, the vendor agrees that maintenance, monitoring, or warranty services will be provided for_____year(s) thereafter.

D **One Time Purchase:** The term of this Contract shall run from the issuance of the Award Document until all of the goods contracted for have been delivered, but in no event will this Contract extend for more than one fiscal year.

D **Other:** See attached.

4. NOTICE TO PROCEED: Vendor shall begin performance of this Contract immediately upon receiving notice to proceed unless otherwise instructed by the Agency. Unless otherwise specified, the fully executed Award Document will be considered notice to proceed.

5. QUANTITIES: The quantities required under this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below.

12] **Open End Contract:** Quantities listed in this Solicitation are approximations only, based on estimates supplied by the Agency. It is understood and agreed that the Contract shall cover the quantities actually ordered for delivery during the term of the Contract, whether more or less than the quantities shown.

12] **Service:** The scope of the service to be provided will be more clearly defined in the specifications included herewith.

D **Combined Service and Goods:** The scope of the service and deliverable goods to be provided will be more clearly defined in the specifications included herewith.

D **One Time Purchase:** This Contract is for the purchase of a set quantity of goods that are identified in the specifications included herewith. Once those items have been delivered, no additional goods may be procured under this Contract without an appropriate change order approved by the Vendor, Agency, Purchasing Division, and Attorney General's office.

6. EMERGENCY PURCHASES: The Purchasing Division Director may authorize the Agency to purchase goods or services in the open market that Vendor would otherwise provide under this Contract if those goods or services are for immediate or expedited delivery in an emergency. Emergencies shall include, but are not limited to, delays in transportation or an unanticipated increase in the volume of work. An emergency purchase in the open market, approved by the Purchasing Division Director, shall not constitute of breach of this Contract and shall not entitle the Vendor to any form of compensation or damages. This provision does not excuse the State from fulfilling its obligations under a One Time Purchase contract.

7. REQUIRED DOCUMENTS : All of the items checked below must be provided to the Purchasing Division by the Vendor as specified below.

D **BID BOND (Construction Only):** Pursuant to the requirements contained in W. Va. Code § 5-22-1(c), All Vendors submitting a bid on a construction project shall furnish a valid bid bond in the amount of five percent (5%) of the total amount of the bid protecting the State of West Virginia. The bid bond must be submittedwith the bid.

D **PERFORMANCE BOND:** The apparent successful Vendor shall provide a performance bond in the amount of 100% of the contract. The performance bond must be received by the Purchasing Division prior to Contractaward.

0 **LABOR/MATERIAL PAYMENT BOND:** The apparent successful Vendor shall provide a labor/material payment bond in the amount of 100% of the Contract value. The labor/material payment bond must be delivered to the Purchasing Division prior o Contract award.

In lieu of the Bid Bond, Performance Bond, and Labor/Material Payment Bond, the Vendor may provide certified checks, cashier's checks, or irrevocable letters of credit. Any

certified check, cashier's check, or irrevocable letter of credit provided in lieu of a bond must be of the same amount and delivered on the same schedule as the bond it replaces. A letter of credit submitted in lieu of a performance and labor/material payment bond will only be allowed for projects under
$100,000. Personal or business checks are not acceptable. Notwithstandingthe foregoing, West Virginia Code § 5-22-1 (d) mandates that a vendor provide a performance and labor/material payment bond for construction projects. Accordingly, substitutions for the performance and labor/material payment bonds for construction projects is not permitted.

D **MAINTENANCE BOND:** The apparent successful Vendor shall provide a two (2) year maintenance bond covering the roofing system. The maintenance bond must be issued and delivered to the Purchasing Division prior to Contract award.

0 **LICENSE(S) /CERTIFICATIONS/ PERMITS:** In addition to anything required under the Section of the General Terms and Conditions entitled Licensing, the apparent successful Vendor shall furnish proof of the following licenses, certifications, and/or permits prior to Contract
award, in a form acceptable to the Purchasing Division.

□

□

□

□

The apparent successful Vendor shall also furnish proof of any additional licenses or certifications contained in the specifications prior to Contract award regardless of whether or not that requirement is listed above.

8. INSURANCE: The apparent successful Vendor shall furnish proof of the insurance identified by a checkmark below and must include the State as an additional insured on each policy prior to Contract award. The insurance coverages identified below must be maintained throughout the life of this contract. Thirty (30) days prior to the expiration of the insurance policies, Vendor shall provide the Agency with proof that the insurance mandated herein has been continued. Vendor must also provide Agency with immediate notice of any changes in its insurance policies, including but not limited to, policy cancelation, policy reduction, or change in insurers. The apparent successful Vendor shall also furnish proof of any additional insurancerequirements contained in the specifications prior to Contract award regardless of whether or not that insurance requirement is listed in this section.

Vendor must maintain:

0 **Commercial General Liability Insurance** in at least an amount of: $1,000,000.00 per occurrence.

0 **Automobile Liability Insurance** in at least an amount of: $1,000,000.00 per occurrence.

0 **Professional/Malpractice/Errors and Omission Insurance** in at least an amount of: ____________________er occurrence.

D **Commercial Crime and Third Party Fidelity Insurance** in an amount of:________________ __ per occurrence.

D **Cyber Liability Insurance** in an amount of: _ _ _ _ _ _ _ _ _ _ _ _ _ per occurrence.

D **Builders Risk Insurance** in an amount equal to 100% of the amount of the Contract.

D **Pollution Insurance** in an amount of: __________________p occurrence.

D **Aircraft Liability** in an amount of:_ _ _ _ _ _ _ _ per occurrence.

□

□

□

□

Notwithstanding anything contained in this section to the contrary, the Director of the Purchasing Division reserves the right to waive the requirement that the State be named as an additional insured on one or more of the Vendor's insurance policies if the Director finds that doing so is in the State's best interest.

9. WORKERS' COMPENSATION INSURANCE: The apparent successful Vendor shall comply with laws relating to workers compensation, shall maintain workers' compensation insurance when required, and shall furnish proof of workers' compensation insurance upon request.

10. [Reserved]

11. LIQUIDATED DAMAGES: This clause shall in no way be considered exclusive and shall not limit the State or Agency's right to pursue any other available remedy.

Vendor shall pay liquidated damages in the amount specified below or as described in the specifications:

□_ _ _ _ _ _ _ _ _ _ _ _ _ _ for _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

D Liquidated Damages Contained in the Specifications

12. ACCEPTANCE: Vendor's signature on its bid, or on the certification and signature page, constitutes an offer to the State that cannot be unilaterally withdrawn, signifies that the product or service proposed by vendor meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise indicated, and signifies acceptance of the terms and conditions contained in the Solicitation unless otherwise indicated.

13. PRICING: The pricing set forth herein is firm for the life of the Contract, unless specified elsewhere within this Solicitation/Contract by the State. A Vendor's inclusion of price adjustment provisions in its bid, without an express authorization from the State in the Solicitation to do so, may result in bid disqualification. Notwithstanding the foregoing, Vendor must extend any publicly advertised sale price to the State and invoice at the lower of the contract price or the publicly advertised saleprice.

14. PAYMENT IN ARREARS: Payment in advance is prohibited under this Contract. Payment may only be made after the delivery and acceptance of goods or services. The Vendor shall submit invoices, in arrears.

15. PAYMENT METHODS: Vendor must accept payment by electronic funds transfer and P-Card. (The State of West Virginia' s Purchasing Card program, administered under contract by a banking institution, processes payment for goods and services through state designated credit cards.)

16. TAXES: The Vendor shall pay any applicable sales, use, personal property or any other taxes arising out of this Contract and the transactions contemplated thereby.
The State of
West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.

17. ADDITIONAL FEES: Vendor is not permitted to charge additional fees or assess additional charges that were not either expressly provided for in the solicitation published by the State of West Virginia or included in the unit price or lump sum bid amount that Vendor is required by the solicitation to provide. Including such fees or charges as notes to the solicitation may result in rejection of vendor's bid. Requesting such fees or charges be paid after the contract has been awarded may result in cancellation of the contract.

18. FUNDING: This Contract shall continue for the term stated herein, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise made available, this Contract becomes void and of no effect beginning on July 1 of the fiscal year for which funding has not been appropriated or otherwise made available.

19. CANCELLATION: The Purchasing Division Director reserves the right to cancel this Contract immediately upon written notice to the vendor if the materials or workmanship supplied do not conform to the specifications contained in the Contract. The Purchasing Division Director may also cancel any purchase or Contract upon 30 days written notice to the Vendor in accordance with West Virginia Code of State Rules§ 148-

1-5.2.b.

20. TIME: Time is of the essence with regard to all matters of time and performance in this Contract.

21. APPLICABLE LAW: This Contract is governed by and interpreted under West Virginia law without giving effect to its choice of law principles. Any information provided in specification manuals, or any other source, verbal or written, which contradicts or violates the West Virginia Constitution, West Virginia Code or West Virginia Code of State Rules is void and of no effect.

22. COMPLIANCE WITH LAWS: Vendor shall comply with all applicable federal, state, and local laws, regulations and ordinances. By submitting a bid, Vendor acknowledges that it has reviewed, understands, and will comply with all applicable laws, regulations, and ordinances.

> **SUBCONTRACTOR COMPLIANCE:** Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to comply with all applicable laws, regulations, and ordinances. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

23. ARBITRATION: Any references made to arbitration contained in this Contract, Vendor's bid, or in any American Institute of Architects documents pertaining to this Contract are hereby deleted, void, and of no effect.

24. MODIFICATIONS: This writing is the parties' final expression of intent. Notwithstanding anything contained in this Contract to the contrary no modification of this Contract shall be binding without mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any change to existing contracts that adds work or changes contract cost, and were not included in the original contract, must be approved by the Purchasing Division and the Attorney General's Office (as to form) prior to the implementation of the change or commencement of work affected by the change.

25. WAIVER: The failure of either party to insist upon a strict performance of any of the terms or provision of this Contract, or to exercise any option, right, or remedy herein contained, shall not be construed as a waiver or a relinquishment for the future of such tenn, provision, option, right, or remedy, but the same shall continue in full force and effect. Any waiver must be expressly stated in writing and signed by the waiving party.

26. SUBSEQUENT FORMS: The terms and conditions contained in this Contract shall supersede any and all subsequent terms and conditions which may appear on any form documents submitted by Vendor to the Agencyor Purchasing Division such as price lists, order forms, invoices, sales agreements, or maintenance agreements, and includes internet websites or other electronic documents. Acceptance or use of Vendor's fonns does not constitute acceptance of the terms and conditions contained thereon.

27. ASSIGNMENT: Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent of the

Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments.

28. WARRANTY: The Vendor expressly warrants that the goods and/or services covered by this Contract will: (a) conform to the specifications, drawings, samples, or other description furnished or specified by the Agency; (b) be merchantable and fit for the purpose intended; and
(c) be free from defect in material and workmanship.

29. STATE EMPLOYEES: State employees are not permitted to utilize this Contract for personal use and the Vendor is prohibited from permitting or facilitating the same.

30. PRIVACY, SECURITY, AND CONFIDENTIALITY: The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable info rmation or other confidential infonnation gained from the Agency, unless the individual who is the subject of the information consents to the disclosurein writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in http://www.state.wv.us/admin/purchase/privacy/default.html.

31. YOUR SUBMISSION IS A PUBLIC DOCUMENT: Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposalopening or award of the contract, as required by the competitive bidding laws of West Virginia Code§§ SA-3-1 et seq., 5-22-1 et seq., and SG-1-1 et seq. and the Freedom of Information Act West Virginia Code§§ 29B-l-l et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "con fidential," " proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.

32. LICENSING: In accordance with West Virginia Code of State Rules § 148-1-6.1.e, Vendor must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State' s Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agency or political subdivision. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Upon request, the Vendor must provide all necessary releases to obtain information to enable the Purchasing Division Director or the Agency to verify that the Vendor is licensed and in good standing with the above entities.

SUBCONTRACTOR COMPLIANCE: Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcon tractors, they too are required to be licensed , in good standing, and up-to-date on all state and local obligations as described in this section. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

33. ANTITRUST: In submitting a bid to, signing a contract with, or accepting a Award Document from any agency of the State of West Virginia, the Vendor agrees to convey, sell, assign, or transfer to the State of West Virginia all rights, title, and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to Vendor.

34. VENDOR CERTIFICATIONS: By signing its bid or entering into this Contract, Vendor certifies (1) that its bid or offer was made without prior understanding, agreement, or connection with any corporation , firm, limited liability company, partnership, person or entity submitting a bid or offer for the same material, supplies, equipment or services; (2) that its bid or offer is in all respects fair and without collusion or fraud; (3) that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; and (4) that it has reviewed this Solicitation in its entirety; understands the requirements, terms and conditions, and other information contained herein.

Vendor' s signature on its bid or offer also affirms that neither it nor its representatives have any interest, nor shall acquire any interest, direct or indirect, which would compromise the performance of its services hereunder. Any such interests shall be promptly presented in detail to the Agency. The individual signing this bid or offer on behalf of Vendor certifies that he or she is authorized by the Vendor to execute this bid or offer or any documents related thereto on
Vendor's behalf; that he or she is authorized to bind the Vendor in a contractual relationship; and that, to the best of his or her knowledge, the Vendor has properly registered with any State agency that may require registration.

35. VENDOR RELATIONSHIP: The relationship of the Vendor to the State shall be that of an independent contractor and no principal-agent relationship or employer-employee relationship is contemplated or created by this Contract. The Vendor as an independent contractor is solely liable for the acts and omissions of its employees and agents. Vendor shall be responsible for selecting, supervising, and compensating any and all individuals employed pursuant to the terms of this Solicitation and resulting contract. Neither the Vendor, nor any employees or subcontractors of the Vendor, shall be deemed to be employees of the State for any purpose whatsoever. Vendor shall be exclusively responsible for payment of employees and contractors for all wages and salaries, taxes, withholding payments, penalties, fees, fringe benefits, professional liability insurance premiums, contributions to insurance and pension, or other deferred compensation plans, including but not limited to, Workers' Compensation and Social Security obligations, licensing fees, etc. and the filing of all necessary documents, forms, and returns pertinent to all of the foregoing.

Vendor shall hold harmless the State, and shall provide the State and Agency with a defense against any and all claims including, but not limited to , the foregoing payments, withholdings, contributions, taxes, Social Security taxes, and employer income tax returns.

36. INDEMNIFICATION: The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction , deliver y, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws incl uding, but not limited to, labor and wage and hour laws.

37. PURCHASING AFFIDAVIT: In accordance with West Virginia Code§§ SA-3-lOa and 5-22-1(i), the State is prohibited from awarding a contract to any bidder that owes a debt to the State or a political subdivision of the State, Vendors are required to sign, notarize, and submit the Purchasing Affidavit to the Purchasing Division affirming under oath that it is not in default on any monetary obligation owed to the state or a political subdivision of the state.

38. ADDITIONAL AGENCY AND LOCAL GOVERNMENT USE: This Contract may be utilized by other agencies, spending units, and political subdivisions of the State of West Virginia; county, municipal , and other local government bodies; and school districts ("Other Government Entities"), provided that both the Other Government Entity and the Vendor agree. Any extension of this Contract to the aforementioned Other Government Entities must be on the same prices, terms, and conditions as those offered and agreed to in this Contract, provided that such extension is in compliance with the applicable laws, rules, and ordinances of the Other Government Entity. A refusal to extend this Contract to the Other Government Entities shall not impact or influence the award of this Contract in any manner.

39. CONFLICT OF INTEREST: Vendor, its officers or members or employees, shall not presently have or acquire an interest, direct or indirect, which would conflict with or compromise the performance of its obligations hereunder. Vendor shall periodically inquire of its officers, members and employees to ensure that a conflict of interest does not arise. Any conflict of interest discovered shall be promptly presented in detail to the Agency.

40. REPORTS: Vendor shall provide the Agency and/or the Purchasing Division with the following reports identified by a checked box below:

0 Such reports as the Agency and/or the Purchasing Division may request. Requested reports may include, but are not limited to, quantities purchased, agencies utilizing the contract, total contract expenditures by agency, etc.

D Quarterly reports detailing the total quantity of purchases in units and dollars, along with a listing of purchases by agenc y. Quarterly reports should be delivered to the Purchasing Division via email at purchasing.reguisitions@wv.gov.

41. BACKGROUND CHECK: In accordance with W. Va. Code§ I5-2D-3 , the Director of the Division of Protective Services shall require any service provider whose employees are regularly employed on the grounds or in the buildings of the Capitol complex or who have access to sensitive or critical information to submit to a fingerprint-based state and federal background inquiry through the state repository. The service provider is responsible for any costs associated with the fingerprint-based state and federal background inquiry.

After the contract for such services has been approved, but before any such employees are permitted to be on the grounds or in the buildings of the Capitol complex or have access to sensitive or critical information, the service provider shall submit a list of all persons who will be physically present and working at the Capitol complex to the Director of the Division of Protective Services for purposes of verifying compliance with this provision. The State reserves the right to prohibit a service provider' s employees from accessing sensitive or critical information or to be present at the Capitol complex based upon results addressed from a criminal background check.

Service providers should contact the West Virginia Division of Protective Services by phone at (304) 558-9911 for more information.

42. PREFERENCE FOR USE OF DOMESTIC STEEL PRODUCTS: Except when authorized by the Director of the Purchasing Division pursuant to W. Va. Code§ 5A-3-56, no contractor may use or supply steel products for a State Contract Project other than those steel products made in the United States. A contractor who uses steel products in violation of this section may be subject to civil penalties pursuant to W. Va. Code§ 5A-3-56. As used in this section:

a. "State Contract Project" means any erection or construction of, or any addition to, alteration of or other improvement to any building or structure, including, but not limited to, roads or highways, or the installation of any heating or cooling or ventilating plants or other equipment, or the supply of and materials for such projects, pursuant to a contract with the State of West Virginia for which bids were solicited on or after June 6, 2001.

b. "Steel Products" means products rolled, formed, shaped, drawn, extruded, forged, cast, fabricated or otherwise similarly processed, or processed by a combination of two or more or such operations, from steel made by the open heath, basic oxygen, electric furnace, Bessemer or other steel making process. The Purchasing Division Director may, in writing, authorize the use of foreign steel products if:

c. The cost for each contract item used does not exceed one tenth of one percent (.1%) of the total contract cost or two thousand five hundred dollars ($2,500.00), whichever is greater. For the purposes of this section, the cost is the value of the steel product as delivered to the project; or

d. The Director of the Purchasing Division determines that specified steel materials are not produced in the United States in sufficient quantity or otherwise are not reasonably available to meet contractrequirements.

43. PREFERENCE FOR USE OF DOMESTIC ALUMINUM, GLASS, AND STEEL: In Accordance with W. Va. Code§ 5-19-1 et seq., and W. Va. CSR§ 148-10-1 et seq., for every contract or subcontract, subject to the limitations contained herein, for the construction, reconstruction,alteration, repair, improvement or maintenance of public works or for the purchase of any item of machinery or equipment to be used at sites of public works, only domestic aluminum, glass or steel products shall be supplied unless the spending officer determines, in writing, after the receipt of offers or bids, (l) that the cost of domestic aluminum, glass or steel products is unreasonable or inconsistent with the public interest of the State of West Virginia, (2) that domestic aluminum, glass or steel products are not produced in sufficient quantities to meet the contract requirements, or (3) the available domestic aluminum, glass, or steel do not meet the contract specifications. This provision only applies to public works contracts awarded in an amount more than fifty thousand dollars ($50,000) or public works contracts that require more than ten thousand pounds of steel products.

The cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than twenty percent (20%) of the bid or offered price for foreign made aluminum, glass, or steel products. If the domestic aluminum, glass or steel products to be supplied or produced in a

"substantial labor surplus area", as defined by the United States Department of Labor, the cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than thirty percent (30%) of the bid or offered price for foreign made aluminum, glass, or steel products. This preference shall be applied to an item of machinery or equipment, as indicated above, when the item is a single unit of equipment or machinery manufactured primarily of aluminum, glass or steel, is part of a public works contract and has the sole purpose or of being a permanent part of a single public works project. This provision does not apply to equipment or machinery purchased by a spending unit for use by that spending unit and not as part of a single public works project.

All bids and offers including domestic aluminum, glass or steel products that exceed bid or offer prices including foreign aluminum, glass or steel products after application of the preferences provided in this provision may be reduced to a price equal to or lower than the lowest bid or offer price for foreign aluminum, glass or steel products plus the applicable preference. If the reduced bid or offer prices are made in writing and supersede the prior bid or offer prices, all bids or offers, including the reduced bid or offer prices, will be reevaluated in accordance with this rule.

44. INTERESTED PARTY SUPPLEMENTAL DISCLOSURE: W. Va. Code§ 6D-1-2 requires that for contracts with an actual or estimated value of at least $1 million, the vendor must submit to the Agency a supplemental disclosure of interested parties reflecting any new or differing interested parties to the contract, which were not included in the original pre- award interested party disclosure, within 30 days following the completion or termination of the contract. A copy of that form is included with this solicitation or can be obtained from the WV Ethics Commission. This requirement does not apply to publicly traded companies listed on a national or international stock exchange. A more detailed definition of interested parties can be obtained from the form referenced above.

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

____

(Name, Title)

(Printed Name and

Title) (Address)

(Phone Number) / (Fax

Number) (email address)

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that I have reviewed this Solicitation in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that I am authorized by the vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on vendor's behalf; that
I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

(Company)

(Authorized Signature) (Representative Name, Title)

(Printed Name and Title of Authorized Representative)

(Date)

(Phone Number) (Fax Number)

<u>SPECIFICAT IONS</u>

1. **PURPOSE AND SCOPE:** The West Virginia Purchasing Division is soliciting bids on behalf of The WV Office of Technology to establish a contract for an EndPoint Detection and Response Software to support approximately two thousand (2,000) endpoints across the state of West Virginia but can be managed centrally. This service will assist in the continuous monitoring and response to advanced cyber security threats.

2. **DEFINITIONS:** The terms listed below shall have the meanings assigned to them

below. Additional definitions can be found in section 2 of the General Terms and Conditions.

2.1 **"Business Hours"** means Monday - Friday 8:00 AM to 5:00 PM EST excluding weekends and Federal and State holidays, which are as follows:

- New Year's Day (January 1)
- Martin Luther King Day (Third Monday in January)
- President's Day (Third Monday in February)
- Memorial Day (Last Monday in May)
- West Virginia Day (June 20)
- Independence Day (July 4)
- Labor Day (First Monday in September)
- Columbus Day (Second Monday in October)
- Veterans Day (November 11)
- Thanksgiving (Fourth Thursday in November)
- Day After Thanksgiving (Fourth Friday in November)
- Christmas Day (December 25)

2.2 **"Contract Services"** means an EndPoint Detection and Response Service to support approximately 2,000 endpoints across the state of WV, as more fully described in these specifications.

2.3 **"EDR"** means EndPoint Detection and Response.

2.4 **"Endpoints"** means an Internet-capable computer hardware device on a TCP/IP network, including desktop computers, laptops, tablets, thin clients, and servers.

2.5 **"FTI"** means an Federal Tax Information.

2.6 **"Pricing Page"** means the pages, contained in wvOASIS or attached hereto as Exhibit A, upon which Vendor should list its proposed price for the Contract Services.

2.7 **"Solicitation"** means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

3. QUALIFICATIONS: Vendor, or Vendor's staff if requirements are inherently limited to individuals rather than corporate entities, shall have the following minimum qualifications:

3.1 The Vendor must be compliant with Internal Revenue Service (IRS) 1075, Section 9.3.1.12 - Remote Access requirements.

3.1.1 IRS 1075, Section 9.3.1.12 states that *"FT] cannot be accessed remotely by agency employees, agents, representatives, or contractors located offthore - outside of the United States* *territories, embassies, or military installations. Further, FT! may not be received, processed, stored, transmitted, or disposed ofby IT systems located offthore."*

3.2 The Vendor must have the ability to provide at a minimum 3-tiered levels of support. Documentation detailing the Vendor's tiered level support must be available upon request. The levels of support must consist of following:

3.2.1 A Customer Service Tier; Initial contact that will provide tier one

3.2.2 Ssupport to include basic troubleshooting.

3.2.3 An Engineering Tier; If tier one troubleshooting is unable to resolve the issue at hand, then it needs to be able to be escalated to an engineer level support.

3.2.4 An Onsite Support Tier; To include any and all subject matter experts applicable to the problem that cannot be fixed remotely.

3.3 The Vendor must provide upon request, examples of at least five (5) successful implementations of their EDR service over last three (3) years.

3.4 The Vendor must provide upon request a dedicated Project Manager and Project Management services during the implementation of the proposed service, including a project plan.

3.4.1 The project plan must include but is not limited to the Work Breakdown Structure, a change management plan, a communication plan, and weekly status report.

4. MANDATORY REQUIREMENTS:

4.1 **Mandatory Contract Services Requirements and Deliverables:** Contract Services must meet or exceed the mandatory requirements listed below.

4.1.1 Contract Item: Endpoint Detection and Response Software

4.1.1.1 Containment & Remediation

4.1.1.2 The Vendor must provide a software and/or service that is capable of supporting a minimum of two thousand (2,000) endpoints throughout the State of West Virginia

- Because of the scalability and simplicity of installation, CrowdStrike has customers with deployments in excess of 500,000 endpoints. Our cloud resources automatically scale based on customer demand, with minimal impact on endpoint resource utilization.
- CrowdStrike platform is SaaS “cloud based”, which removes all the traditional legacy architecture issues/complexity. No consoles to manage and no hardware and storage to be operated, managed or maintained by the client.

- Falcon Host is delivered as an MSI package for Windows, and can be deployed using any software deployment tool such as SCCM. There is no reboot required at installation, and there are no user-mode components (such as alerts or popups) so deployment is very straight forward. Most customers are fully (and successfully) deployed in production in a matter of hours or days.
- At CrowdStrike we pride ourselves in having best time to value with some of our clients deploying 77,000 endpoints in one day, other 120,000 in two weekends.
- Deploying Falcon Prevent across your environment is easy, fast and safe. We provide tips and best practices for rapid deployment of Falcon Prevent, as well as guidance on how to replace your legacy antivirus with Falcon Prevent.
- Deploying traditional security products can often take weeks or even months. CrowdStrike regularly has customers deploy tens of thousands of sensors in a day, during business hours, with no interruption to operations or helpdesk calls. There is no hardware to maintain or deploy. There is no need to reboot a system after an install, in fact, the entire process is invisible to the end user. Falcon Prevent can be deployed to Windows, Mac and Linux systems providing broad coverage on critical systems. Once deployed, Falcon Prevent can update on its own, eliminating the need for maintenance windows and downtime.
- Some customers would like to control this aspect. Creating release groups allows customers this level of granularity and control over their environment.
- The first cloud-native Endpoint Protection Platform which eliminates complexity and simplifies deployment to drive down operational cost.
- A single lightweight agent works everywhere, including virtual machines and data centers — providing protection even when endpoints are offline. Delivers everything you need to stop breaches — providing maximum effectiveness on day one
- AI Powered. Harnesses the power of big data and artificial intelligence to empower your team with instant visibility

4.1.1.3 The Vendor must provide a software and/or service that can be centrally managed by a West Virginia Office of Technology Administrator.

- CrowdStrike Falcon Platform UI presents in real-time detections/preventions in a simple to understand graphically rich format, which means you don't have to dig around the console to piece together different events involved in an attack. Our process timeline shows an entire attack in sequence with activity before the attack occurred and after it occurred. We also offer an interactive process visualization that allows you to pivot on different activity involved in an attack. Analysts can drill down into hosts, processes, and down to file reads by a process.
  All real-time event data is centralized in the cloud and available for reporting and analysis. The platform has as well the ability for reporting, with various dashboards available. Email notification and integration with SIEM can be used as well as a vehicle to consume alerts.

- Mapping alerts to the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&Ck) Framework allows you to understand even the most complex detections at a glance,

- shortening the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.

- The Falcon console uses colors to indicate the detection name, description, severity of a detection scenario. For example, are dweb exploit represents a high severity web exploit. Colors make it easy to identify and prioritize security events.
- The Falcon console allows analyst to filter events based on many attributes such as Severity, Scenario, Objective, Tactics, Techniques and many others. In addition, events can be grouped by similar attributes to provide further prioritization.

4.1.1.4 The Vendor must provide a software and/or service that shall feature the following:

4.1.1.4.1 Automatically restrict potentially malicious activity to within an isolation container.

- Falcon uses multiple methods to prevent and detect malware. Those methods include machine learning, exploit blocking, blacklisting and indicators of attack. This unified combination of methods protects you against known malware, unknown malware, script-based attacks, file-less malware and others.

4.1.1.4.2 Automatically isolate applications interacting with untrusted content from more trusted portions of the device outside the container.

- Data gathered by the sensor is then transmitted continuously from the sensor to CrowdStrike's Advanced Threat Intelligence Cloud, where CrowdStrike analyzes and draws links between events across the entire Falcon sensor community. These behavioral patterns are detected in real time via CrowdStrike's Threat Graph data model, allowing analysts to detect new attacks, whether the attacks use malware or not.

4.1.1.4.3 Automatically detect and isolate potentially malicious code behavior.

4.1.1.4.4 Continuously detect, and isolate threats based on machine learning, behavioral analytics, and custom detection rules.

- Machine learning (ML) is used for pre-execution prevention. CrowdStrike employs sophisticated machine learning algorithms that can analyze millions of file characteristics to determine if a file is malicious. This signature-less technology enables CrowdStrike to detect and block both known and unknown malware.

- First, we can block known malware by leveraging machine learning which allows us to have complex cloud-based patterns that can easily be fine-tuned in the cloud instead of the endpoint.

- This is a much more powerful approach instead of relying on one single anti- virus vendor in the entire environment. Instead we are relying on the collective intelligence of the anti-malware community and proprietary machine learning. Regardless of which anti-virus product you are using, it is mathematically impossible that they will always be first to detect and prevent a new piece of malware. Which is why it makes sense to leverage more powerful machine learning that takes many factors into account instead of just static signatures. This rules out false positives and ultimately delivers a high confidence block on any file that is attempting to execute that meets our confidence criteria.

- Falcon Endpoint Protection agent evaluate events in real-time, by keeping track of parent-child relationship between processes agent is able to understand the context of the event, detect malicious activities and modify severity based on the action and ultimately take a preventative action when necessary. Pertaining to Machine learning flow is dependent on endpoint connection to CrowdStrike cloud, in case of Airplane mode operation ML on sensor will take the precedent otherwise evaluation will start typically with Cloud + On sensor, please keep in mind cloud evaluation does not require file transfer to the cloud. IOAs and ML will run in parallel so is the other detection capabilities such as CrowdStrike IOCs, client specific IOCs and finally

- In addition, we deliver comprehensive exploit blocking on the endpoint for non-malware attacks such as ASLR, Buffer Overflows and other common Microsoft exploits. Again, this focuses on stopping attacks before an adversary makes into your environment not just alerting you with a detection after the fact.

4.1.1.4.5 Automatically capture necessary event details on all malicious activity, including but not limited to ports and protocols in use, running executables and services, and browser plugins occurring within the isolation container to support retrospective post-event analysis, threat analysis, and situational awareness.

- Observe every move in real time: Immediate visibility allows you to view the activities as if you were "shoulder surfing" the adversary.
- Capture critical details for threat hunting and forensic investigations: Falcon Insight kernel-mode driver captures over 400 raw events and related information necessary to retrace incidents.
- Get answers in seconds: The CrowdStrike Threat Graph™ database stores event data and answers queries in five seconds or less, even across billions of events.
- Recall for up to 90 days: Falcon Insight provides a complete record of endpoint activity over time, whether your environment consists of fewer than 100 endpoints or more than 500,000

4.1.1.4.6 Be configurable to control the ability of applications running within the isolation container to access only specified system resources.

- CrowdStrike Falcon is a SaaS-based, next generation endpoint protection solution that provides advanced detection, prevention, monitoring and search capabilities, allowing analysts to defend against sophisticated threats and adversaries. Falcon offers remote visibility across endpoints throughout an environment, enabling instant access to the "who, what, when, where, and how" of an attack.

4.1.1.4.7 Automatically eliminate and report all isolation container artifacts of compromise and intrusion remnants.

- CrowdStrike supports a quarantine option for malware-based events prevented. On Windows and Mac hosts, the Falcon sensor can quarantine suspicious files based on your prevention policies. When the Falcon sensor detects a suspicious file attempting to run, the file is encoded, renamed, and moved into a quarantine directory on its host. To use quarantining, you first enable it via a prevention policy. Then, you can use the Falcon console to view and take action on quarantined files. Detection data is available within the console for 90 days. Forensic data retention options include 7, 15, 30, 60 and 90 day options.

- Falcon Insight is a simple and powerful EDR solution that adapts to your needs, growth and security status. Falcon Insight is a module of the CrowdStrike Falcon endpoint protection platform. Falcon Insight acts like a DVR, recording and automatically analyzing activity on the endpoint to catch incidents that evade prevention measures. Insight uses IOAs (indicators of attack) to automatically identify attacker behavior and sends prioritized alerts to the Falcon UI, eliminating time-consuming research and manual searches.

- The CrowdStrike Threat Graph database stores event data and answers queries in five seconds or less, even across billions of events.

- Falcon Sandbox malware analysis gives you complete visibility into advanced and unknown threats.
    - Hybrid Analysis: This combines runtime data, static analysis and memory dump analysis to extract all possible execution pathways even for the most evasive malware. In combination with extensive pre- and post-execution analysis, Falcon Sandbox extracts more IOCs than any other competing sandbox solution. All data extracted from the Hybrid Analysis engine is processed automatically and integrated into the Falcon Sandbox reports.

    - Falcon Sandbox includes state-of-the-art anti-sandbox detection technology. The file monitoring runs in the kernel and cannot be observed by user-mode applications. CrowdStrike doesn't use an agent that can be easily identified by malware and continuously tests each release to ensure Falcon Sandbox is nearly undetectable by malware using even the most sophisticated sandbox detection techniques.
    - Environmental Customization: Take control of how malware is detonated by configuring common settings that malware uses to attempt to hide from sandbox analysis, such as date/time, environmental variables, user behaviors and more.
    - Analysis Reports: Easy to understand reports make every analyst at every level more effective in their roles. The analysis is layered, providing security teams with practical guidance for threat prioritization and response, enabling incident response teams to threat hunt and forensic teams to drill-down for deep analysis into memory captures and stack traces.
    - Broad File Support: Falcon Sandbox supports Windows, Linux and Android (static analysis only) operating systems. In addition, Falcon Sandbox analyzes over 40 different file types that include a wide variety of executables, document and image formats, and script and archive files.

    - Malware Search: Falcon Sandbox will automatically search the industry's largest malware search engine to find related samples and within seconds expand the analysis to include all files. This unique capability provides analysts with a deeper understanding of the attack and a larger set of IOCs that can be used to better protect the organization.
    - Immediate Triage: Falcon Sandbox provides threat scoring and incident response summaries to immediately triage and eradicate malware. In addition, analysis reports are enriched with information and IOCs from CrowdStrike Falcon MalQuery™ and CrowdStrike Falcon Intelligence™, providing the necessary context to make faster, better decisions.
    - Easy Integration: It includes an easy- to-use REST API, pre-built integrations and support for indicator sharing formats including STIX, OpenIOC, MAEC, MISP, and XML/JSON. This enables users to delivers Falcon Sandbox results with SIEMs, TIPs and orchestration systems.
    - Flexible Deployment: You can choose between a cloud or on-premises version of Falcon Sandbox. The cloud option provides immediate time-to-value and reduced infrastructure costs, while the on-premises version enables users to lock down and process samples solely within their environment. Both options

provide a secure and scalable sandbox environment.

4.1.1.4.8 Provide continual verification of the integrity of the isolation container to ensure there 1s no unauthorized/malicious access or persistent modification

- Script based and other fileless attacks are on the rise because they can avoid detection by both new and old detection capabilities. CrowdStrike utilizes many types of detections methods to both identify and stop the broad range of attack vectors utilized today.
- Falcon uses multiple methods to prevent and detect known exploits. These methods include machine learning, exploit blocking, blacklisting, and Indicators of Attack (IOA). This unified combination of methods protects you against known malware, unknown malware and file-less attacks
- There are cases when you might want to block applications because you are certain that you never want them to run in your environment. Falcon allows you to upload hashes from your own black or white lists.

- Attacks that forego the use of malware in favor of more subtle techniques like PowerShell and other script based attacks have seen an uptick in popularity. These attacks often avoid detection by traditional AV solutions. CrowdStrike uses behavioral IOAs (Indicators of attack) to determine if the intention of a series of actions is malicious or legitimate, regardless of whether these actions are generated from PowerShell or other means. This approach provides a unique and proactive capability to defend against attacks that use PowerShell.
- IOAs observe the sequences of PowerShell commands — and it doesn't matter if a series of actions was started from a specific folder, a specific user, or via a CLI or a script. IOAs are concerned with the actions performed, their relation to each other, their sequence and their dependencies, recognizing them as indicators of the true intentions and goals behind a sequence of commands. IOAs are not focused on the specific tools that attackers use, making them a breakthrough defense against the malicious use of PowerShell or the use of any legitimate application for nefarious purposes.

4.1.1.4.9 Automatically report potentially malicious events detected within the isolation container and provide actionable information.

- Observe every move in real time: Immediate visibility allows you to view the activities as if you were "shoulder surfing" the adversary.
- Capture critical details for threat hunting and forensic investigations: Falcon Insight kernel-mode driver captures over 400 raw events and related information necessary to retrace incidents.
- Get answers in seconds: The CrowdStrike Threat Graph™ database stores event data and answers queries in five seconds or less, even across billions of events. Recall for up to 90 days: Falcon Insight provides a complete record of endpoint activity over time, whether your environment consists of fewer than 100 endpoints or more than 500,000

4.1.1.4.10 Be capable of containing operating system kernel-level vulnerability exploitation.

- CrowdStrike developed a sophisticated and easy deployed exploit mitigation layers to prevent exploit techniques such as:
  - Force ASLR
  - Force DEP
  - Heap Spray Preallocation
  - Null Page allocation

  - SHE Overwrite Protection
  - Untrusted Font loading
  - Remote Library loading

- CrowdStrike® Falcon Spotlight™ offers security teams a real-time assessment of vulnerability exposure on their endpoints that is always current. Falcon Spotlight's native integration into the CrowdStrike Falcon® platform enables customers to operate vulnerability assessment within a complete endpoint protection framework. Falcon Spotlight adds preparation and readiness to the unparalleled prevention, detection and response provided by the Falcon platform, resulting in a stronger security posture and unprecedented breach protection.
- Integrated Protection: Spotlight is a key part of CrowdStrike's comprehensive and unified endpoint protection platform. With Spotlight and the Falcon platform, not only can you see your security gaps, you see which gaps your adversary is targeting, arming you with the proactive protection you need to block advanced attacks.

- Comprehensive Visibility: Spotlight requires no scanners to deploy and manage and no new agents — just turn it on and start seeing results. Spotlight gives you visibility across your enterprise, whether endpoints are physical or virtual, on- or off-premises, or on-the-move. You receive unparalleled visibility into vulnerabilities across your distributed enterprise without compromise.
- Effortless: Spotlight delivers always up-to date information seamlessly, putting it into the hands of security analysts. This helps you improve response time and reduces the effort required to understand your security posture and become more proactive. Zero-impact: CrowdStrike's cloud-native architecture enables constant
- visibility into endpoint vulnerabilities without the need for cumbersome and resource intensive network or host scans.

4.1.1.4.11 Provide options for configurable automated or manual remediation actions in response to detected potentially malicious events.

- Real Time Response is a feature that empowers incident responders with deep access to systems across the distributed enterprise. It provides the enhanced visibility necessary to fully understand emerging threats and the power to directly remediate. This helps to dramatically reduce the time needed to respond to attacks and the likelihood of an attack becoming a costly breach. It does all this with zero impact on performance while leveraging existing sensors and cloud infrastructure.
- Real Time Response It offers customers a set of built-in commands to execute against systems during a security investigation. By leveraging the existing Falcon sensor, cloud and console, CrowdStrike is able to deliver Real Time Response capabilities to systems anywhere in the world, with zero incremental cost in terms of performance or infrastructure.

4.1.1.5 Reporting & Monitoring

- Threat hunting is a process that augments traditional security solutions to look for abnormalities within a client's environment.
- Our proactive threat hunters will work with customers to identify their crown jewel assets and critical concerns. They use this customer input to create fully tailored threat hunts and customized EDR detections.
- Customized threat hunt reports
- IBM proprietary Threat Hunt Library
- Proactive and hypothesis-driven in nature
- IBM intelligence
- Quarterly briefings and hunt workshops
- 8x5 service, available during US business hours
- Can operate standalone or in conjunction with Alert Monitoring team

4.1.1.6 The Vendor must provide a software or service that shall interoperate with event monitoring and correlation systems to facilitate aggregated situational awareness.

- Designed from the ground up to deliver best-of-breed security offerings, the Falcon Platform offers partners an open framework for the development and deployment of security services that defend against all types of attacks and share threat data and actor profiles — all delivered from a superior native cloud-based architecture.
- Falcon Streaming API — Obtain a near real-time stream of detections, alerts and audit events. Can be ingested into a SIEM for correlation and triage.
- Falcon Data Replicator API — Complete event data which can be ingested into local data warehouses or logging applications.
- Falcon Threat Graph API — See the relationships between indicators of compromise (IOCs), devices, and processes. Visualize relationships with tools such as Maltego.
- Falcon Query API — Query the Falcon platform to search for indicators of attack (IOAs) and IOCs
- Falcon Orchestrator — Provides enhanced workflow automation and remediation capabilities using the Falcon platform. This application improves the overall effectiveness and efficiency of security and IT teams in conducting their security practices and operations in the areas of account containment, file extraction, remediation, asset monitoring and forensics. Falcon Orchestrator is available as an open source application for SOC analysts.
- SIEM Connector - Customers can forward CrowdStrike Falcon events to their SIEM using the Falcon SIEM Connector. The Falcon SIEM Connector enables integration with most SIEM offerings, such as HP ArcSight, IBM QRadar, and Splunk. Additionally, the Falcon Streaming API is available to customers who wish to build their own custom integration. The application automatically connects to the CrowdStrike Falcon platform, managing and normalizing the data into formats that are immediately usable by SIEMs such as JSON, CEF, and LEEF.
- Community Tools — A collection of resources encompassing vulnerability scanning, forensic collection, deobfuscation, and process inspection
- Github repository — A collection of scripts, source code, libraries and tools covering a variety of security and CrowdStrike-related areas.

4.1.1.7 The software shall support open standards for automated threat information sharing.

- The Falcon SIEM Connector automatically connects to the CrowdStrike Cloud and normalizes the data in formats that are immediately usable by SIEMs: JSON, Syslog, CEF (common event format) or LEEF (log event extended format).

4.1.1.8 The software shall provide integrated and customizable search with, at minimum, the ability to search data from all systems for information relevant to an incident investigation or risk analysis.

- Falcon Insight is a simple and powerful EDR solution that adapts to your needs, growth and security status. Falcon Insight is a module of the CrowdStrike Falcon endpoint protection platform. Falcon Insight acts like a DVR, recording and automatically analyzing activity on the endpoint to catch incidents that evade prevention measures. Insight uses IOAs (indicators of attack) to automatically identify attacker behavior and sends prioritized alerts to the Falcon UI, eliminating time-consuming research and manual searches. The CrowdStrike Threat Graph database stores event data and answers queries in five seconds or less, even across billions of events.

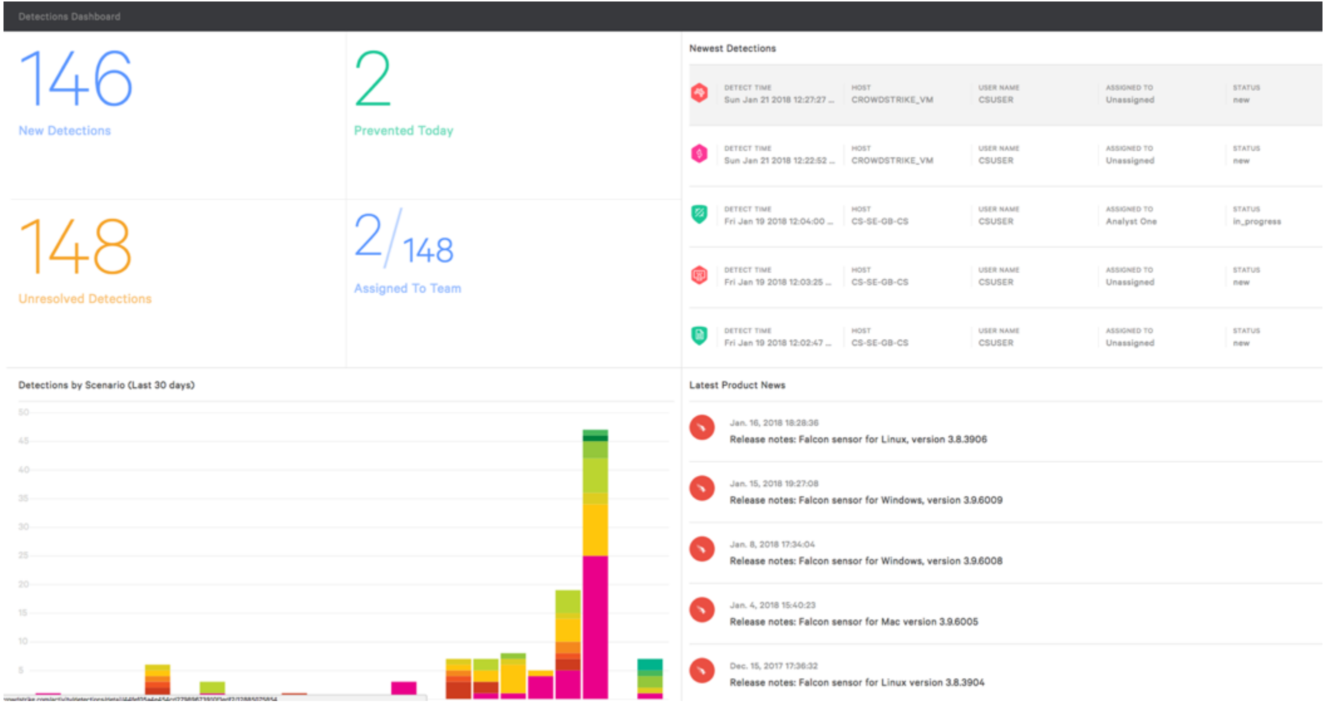
4.1.1.9 The software shall have the ability to execute manual and scheduled scans of specified systems for indicators derived from threat intelligence or other sources.

- The CrowdStrike Falcon platform is pioneering cloud-delivered endpoint protection. It both delivers and unifies IT Hygiene, next-generation antivirus, endpoint detection and response (EDR), and threat intelligence — all delivered via a single lightweight agent. Falcon Endpoint Protection agent is extremely lightweight and installs in under 5 seconds, no reboot is required, there is no active disk scanning on the endpoint so there is no DISK IO impact. Also, the installation process is the same whether you are installing on a workstation, server, laptop, virtual instances on premise or virtual instances in the cloud.

4.1.1.10 The software shall provide integrated analytics (including visualization) and support the creation of custom analytics, in order to identify anomalous endpoint behaviors, support incident investigation, and perform event analysis.

- CrowdStrike Falcon Platform UI presents in real-time detections/preventions in a simple to understand graphically rich format, which means you don't have to dig around the console to piece together different events involved in an attack. Our process timeline shows an entire attack in sequence with activity before the attack occurred and after it occurred. We also offer an interactive process visualization that allows you to pivot on different activity involved in an attack. Analysts can drill down into hosts, processes, and down to file reads by a process. All real-time event data is centralized in the cloud and available for reporting and analysis. The platform has as well the ability for reporting, with various dashboards available. Email notification and integration with SIEM can be used as well as a vehicle to consume alerts.
- Mapping alerts to the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&Ck) Framework allows you to understand even the most complex detections at a glance, shortening the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.
- The Falcon console uses colors to indicate the detection name, description, severity of a detection scenario. For example, are dweb exploit represents a high severity web exploit. Colors make it easy to identify and prioritize security events.
- The Falcon console allows analyst to filter events based on many attributes such as Severity, Scenario, Objective, Tactics, Techniques and many others. In addition, events can be grouped by similar attributes to provide further prioritization.

Detection Dashboard



Detections Dashboard

146 New Detections

2 Prevented Today

148 Unresolved Detections

2/148 Assigned To Team

Newest Detections

DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
Sun Jan 21 2018 12:27:27 ...	CROWDSTRIKE_VM	CSUSER	Unassigned	new
Sun Jan 21 2018 12:22:52 ...	CROWDSTRIKE_VM	CSUSER	Unassigned	new
Fri Jan 19 2018 12:04:00 ...	CS-SE-GB-CS	CSUSER	Analyst One	in_progress
Fri Jan 19 2018 12:03:25 ...	CS-SE-GB-CS	CSUSER	Unassigned	new
Fri Jan 19 2018 12:02:47 ...	CS-SE-GB-CS	CSUSER	Unassigned	new

Detections by Scenario (Last 30 days)

Latest Product News

Jan. 16, 2018 18:28:36
Release notes: Falcon sensor for Linux, version 3.8.3906

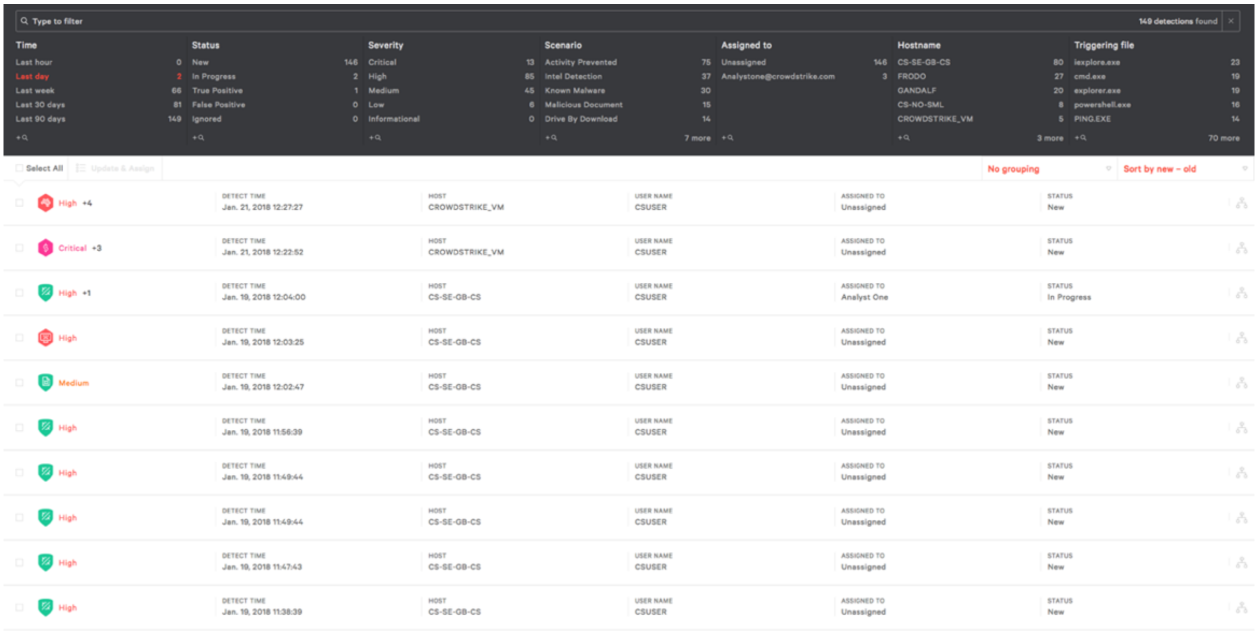
Jan. 15, 2018 19:27:08
Release notes: Falcon sensor for Windows, version 3.9.6009

Jan. 8, 2018 17:34:04
Release notes: Falcon sensor for Windows, version 3.9.6008

Jan. 4, 2018 15:40:23
Release notes: Falcon sensor for Mac version 3.9.6005

Dec. 15, 2017 17:36:32
Release notes: Falcon sensor for Linux version 3.8.3904

Alert (detection/Prevention) details



Type to filter — 149 detections found

Time		Status		Severity		Scenario		Assigned to		Hostname		Triggering file	
Last hour	0	New	146	Critical	13	Activity Prevented	75	Unassigned	146	CS-SE-GB-CS	80	iexplore.exe	23
Last day	2	In Progress	2	High	85	Intel Detection	37	Analystone@crowdstrike.com	3	FRODO	27	cmd.exe	19
Last week	66	True Positive	1	Medium	45	Known Malware	30			GANDALF	20	explorer.exe	19
Last 30 days	81	False Positive	0	Low	6	Malicious Document	15			CS-NO-SML	8	powershell.exe	16
Last 90 days	149	Ignored	0	Informational	0	Drive By Download	14			CROWDSTRIKE_VM	5	PING.EXE	14
							7 more				3 more		70 more

□ Select All Update & Assign — No grouping — Sort by new – old

	DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
□ High +4	Jan. 21, 2018 12:27:27	CROWDSTRIKE_VM	CSUSER	Unassigned	New
□ Critical +3	Jan. 21, 2018 12:22:52	CROWDSTRIKE_VM	CSUSER	Unassigned	New
□ High +1	Jan. 19, 2018 12:04:00	CS-SE-GB-CS	CSUSER	Analyst One	In Progress
□ High	Jan. 19, 2018 12:03:25	CS-SE-GB-CS	CSUSER	Unassigned	New
□ Medium	Jan. 19, 2018 12:02:47	CS-SE-GB-CS	CSUSER	Unassigned	New
□ High	Jan. 19, 2018 11:56:39	CS-SE-GB-CS	CSUSER	Unassigned	New
□ High	Jan. 19, 2018 11:49:44	CS-SE-GB-CS	CSUSER	Unassigned	New
□ High	Jan. 19, 2018 11:49:44	CS-SE-GB-CS	CSUSER	Unassigned	New
□ High	Jan. 19, 2018 11:47:43	CS-SE-GB-CS	CSUSER	Unassigned	New
□ High	Jan. 19, 2018 11:38:39	CS-SE-GB-CS	CSUSER	Unassigned	New

4.1.1.1.11 The software shall allow administrative functions to be delegated to users based on roles/permissions and or groupings of endpoints they are responsible for managing.

- CrowdStrike platform offers the ability to assign different roles to users. Account's roles determine permissions or access to features in the Falcon console.

- In order to grant access to features you want; you can assign multiple roles to a single user. Each user must have at least one role. A user can access a feature if at least one of their roles grants them access.

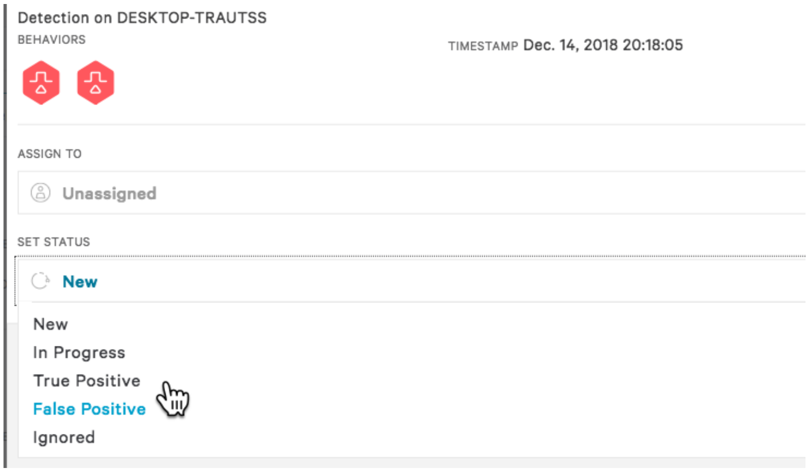
4.1.1.12 The software shall support delegation (i.e., user-specified) of who can access/view collected endpoint data.

Here some of the roles available:

- Falcon Administrator can perform all actions in the Falcon console.
- Falcon Security Lead can manage detections, manage quarantined files, and reset users' credentials.
- Falcon Analyst can manage detections and quarantined files.
- Falcon Analyst - Read Only can view detections.
- Quarantine Manager can manage quarantined files
- Endpoint Manager can manage sensor deployment and sensor update policy settings.
- Prevention Hashes Manager can manage hash blacklists and whitelists for prevention policies.

4.1.1.13 The software shall have the capability to be tuned/configured to reduce alerts resulting from false positives.

- False positives can be marked as such within a dropdown option (as seen below):



Detection on DESKTOP-TRAUTSS

BEHAVIORS

TIMESTAMP Dec. 14, 2018 20:18:05

ASSIGN TO

Unassigned

SET STATUS

New

New
In Progress
True Positive
False Positive
Ignored

- CrowdStrike Falcon leverages machine learning and behavioral analytics, trained on more than 1 trillion security events that the platform processes every week, to enable reliable prevention, detection and mitigation and response to all threats, including sophisticated malware-free intrusions. The results show that CrowdStrike Falcon stands alone in its ability to uncover hands-on-keyboard adversary activity across the entire ATT&CK framework, from the Initial Access stage all the way to Exfiltration and through Command & Control.
- Gartner - CROWDSTRIKE SCORES HIGHEST IN CRITICAL CAPABILITIES FOR ENDPOINT PROTECTION AMONG “TYPE A” ORGANIZATIONS
- Forrester - CROWDSTRIKE A LEADER IN 2018 WAVE REPORTS FOR ENDPOINT SECURITY SUITES AND ENDPOINT DETECTION & RESPONSE
- A false alarm test done with common business software was also performed. As expected,

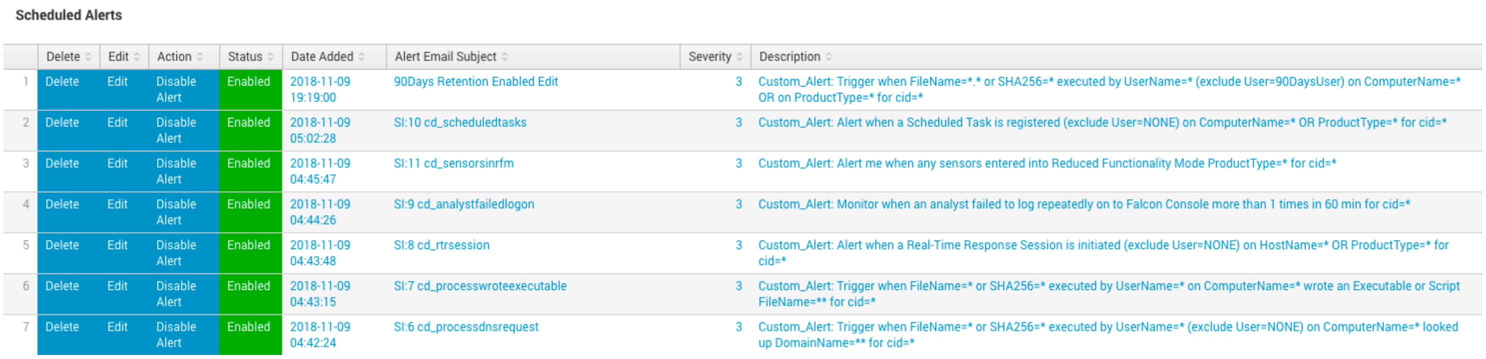
CrowdStrike had zero false alarms on common business software

4.1.1.14 The software shall provide configurable alerting based upon administrator defined criteria.

- Scheduling a Custom Alert for your environment consists of three steps: choosing the template you'd like to configure, previewing the search results, then scheduling the alert. Previewing the results helps you see what your results are found before you schedule the alert. Adjust your search parameters as needed until you're satisfied with the activity being found.

- Up to 50 different custom alerts can be scheduled for your environment at one time.

- Scheduled alerts can be edited, disabled, or re-enabled under Scheduled Alerts. Modify a scheduled alert to expand or narrow its search parameters. We recommend entering multiple search parameters in one Custom Alert instead of creating many similar alerts. Duplicate alerts are not allowed.



Scheduled Alerts

	Delete	Edit	Action	Status	Date Added	Alert Email Subject	Severity	Description
1	Delete	Edit	Disable Alert	Enabled	2018-11-09 19:19:00	90Days Retention Enabled Edit	3	Custom_Alert: Trigger when FileName=*.* or SHA256=* executed by UserName=* (exclude User=90DaysUser) on ComputerName=* OR on ProductType=* for cid=*
2	Delete	Edit	Disable Alert	Enabled	2018-11-09 05:02:28	SI:10 cd_scheduledtasks	3	Custom_Alert: Alert when a Scheduled Task is registered (exclude User=NONE) on ComputerName=* OR ProductType=* for cid=*
3	Delete	Edit	Disable Alert	Enabled	2018-11-09 04:45:47	SI:11 cd_sensorsinrfm	3	Custom_Alert: Alert me when any sensors entered into Reduced Functionality Mode ProductType=* for cid=*
4	Delete	Edit	Disable Alert	Enabled	2018-11-09 04:44:26	SI:9 cd_analystfailedlogon	3	Custom_Alert: Monitor when an analyst failed to log repeatedly on to Falcon Console more than 1 times in 60 min for cid=*
5	Delete	Edit	Disable Alert	Enabled	2018-11-09 04:43:48	SI:8 cd_rtrsession	3	Custom_Alert: Alert when a Real-Time Response Session is initiated (exclude User=NONE) on HostName=* OR ProductType=* for cid=*
6	Delete	Edit	Disable Alert	Enabled	2018-11-09 04:43:15	SI:7 cd_processwroteexecutable	3	Custom_Alert: Trigger when FileName=* or SHA256=* executed by UserName=* on ComputerName=* wrote an Executable or Script FileName=** for cid=*
7	Delete	Edit	Disable Alert	Enabled	2018-11-09 04:42:24	SI:6 cd_processdnsrequest	3	Custom_Alert: Trigger when FileName=* or SHA256=* executed by UserName=* (exclude User=NONE) on ComputerName=* looked up DomainName=** for cid=*

4.1.1.15 The software shall send alerts at administrator-definable intervals.

The administrator will receive new detection email alert from the administrative console.

4.1.1.16 The software shall provide the ability to automatically discover and alert on previously unknown external and/or internal hardware/peripheral devices (such as storage) connected to endpoints for the purpose of retrospective/post-event analysis.

- Discover devices automatically - Gain continuous insight into USB devices across your organization, including those not covered by a policy. Falcon Device Control automatically reports device type (e.g. mass storage, human interface, etc.) with manufacturer, product name, and serial number. You have visibility into all devices operating over the USB bus, including internal/non-removable USB devices and those not categorized as USB by Windows, such as Bluetooth.
- Immediately see which devices are used in your environment and how they are being used at a glance via usage dashboards. Falcon Device Control provides insight into specific files copied to a removable drive, processes executed from USB storage, users, and hosts where USB devices were used.

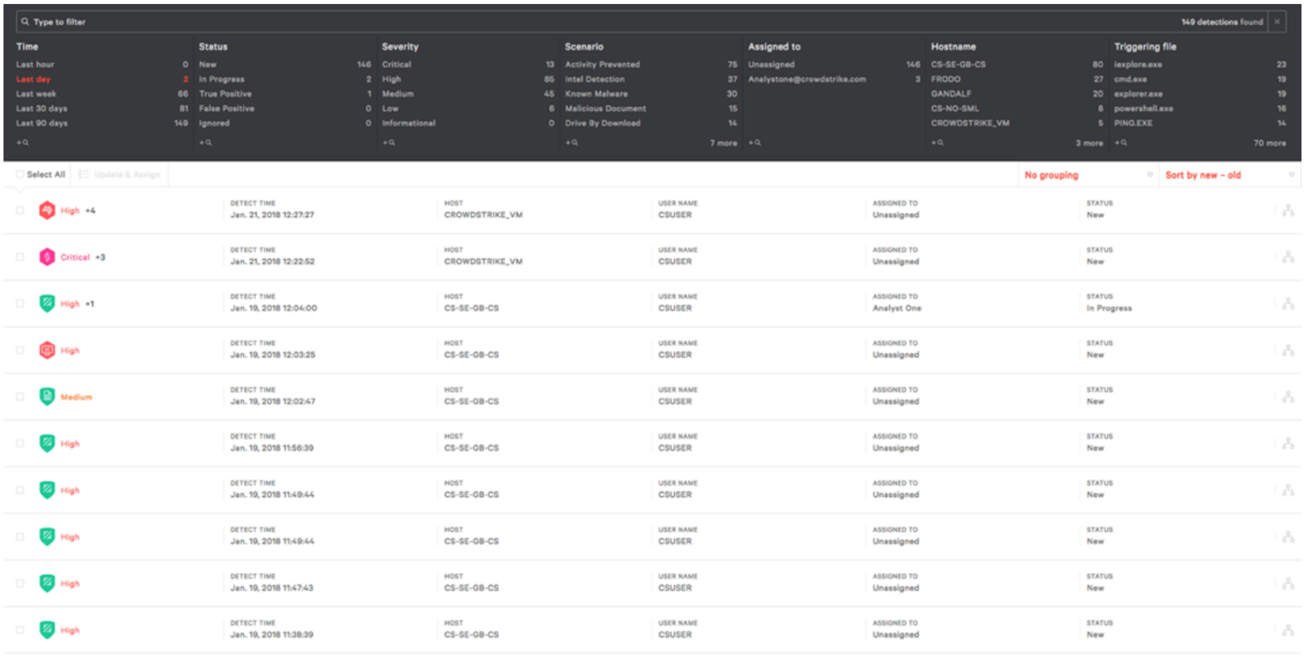
- Falcon Device Control provides fast and powerful real-time and historical search capabilities. Examine your environment for vital information such as the devices used on a specific machine and file writes to mass storage.
- Strict policy enforcement. Define device control policies for endpoint groups, whitelist and blacklist devices by class, vendor, product serial number and/or specific device ID. Define device control policies for endpoints both on and offline.
- See the impact of policies before implementing them. Alerts and dashboards allow you to see how your policies will impact users before rolling them out.
- Define granular policies for drives. Allows read/write or read-only access, while blocking execution of applications on USB drives.
- Monitor files written to storage. Track data moving from your endpoints to storage, giving you visibility into what's being copied to devices.
- Automatically get device information for quick and easy policy creation and management workflows. Falcon Device Control automatically obtains devices' vendor, class model and serial number, without requiring the use of external tools or device managers, allowing you to create policies for all devices being used in your environment.

- As a 100 percent cloud managed and delivered solution, Falcon Device Control is enabled via the same lightweight Falcon agent, managed by the same console, and fully integrated with the Falcon platform.
- Immediate implementation and management. Falcon Device Control hits the ground running and is operational in minutes.

4.1.1.17 The software shall generate reports based on pre-saved user-defined formats and datasets to facilitate rapid analysis, decision making, and follow-up actions following events.

- Falcon UI offers a multitude of predefined dashboards that will give you the tools to facilitate rapid analysis and decision making.

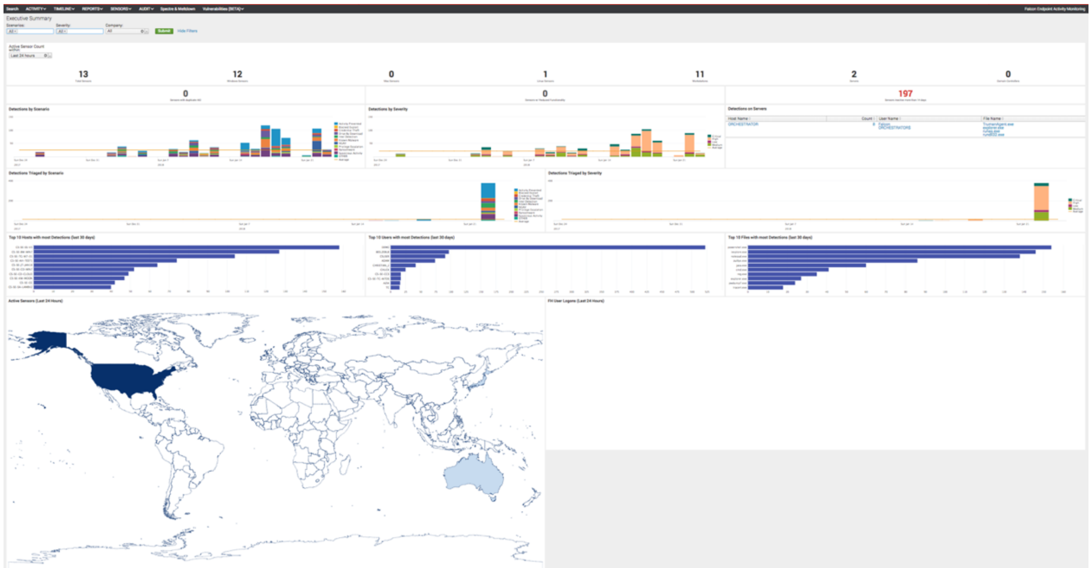
Alert (detection/Prevention) details



Time		Status		Severity		Scenario		Assigned to		Hostname		Triggering file	
Last hour	0	New	146	Critical	13	Activity Prevented	75	Unassigned	146	CS-SE-GB-CS	80	iexplore.exe	23
Last day	2	In Progress	2	High	85	Intel Detection	37	Analystone@crowdstrike.com	3	FRODO	27	cmd.exe	19
Last week	66	True Positive	1	Medium	45	Known Malware	30			GANDALF	20	explorer.exe	19
Last 30 days	81	False Positive	0	Low	6	Malicious Document	15			CS-NO-SML	8	powershell.exe	16
Last 90 days	149	Ignored	0	Informational	0	Drive By Download	14			CROWDSTRIKE_VM	5	PING.EXE	14
							7 more				3 more		70 more

	DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
High +4	Jan. 21, 2018 12:27:27	CROWDSTRIKE_VM	CSUSER	Unassigned	New
Critical +3	Jan. 21, 2018 12:22:52	CROWDSTRIKE_VM	CSUSER	Unassigned	New
High +1	Jan. 19, 2018 12:04:00	CS-SE-GB-CS	CSUSER	Analyst One	In Progress
High	Jan. 19, 2018 12:03:25	CS-SE-GB-CS	CSUSER	Unassigned	New
Medium	Jan. 19, 2018 12:02:47	CS-SE-GB-CS	CSUSER	Unassigned	New
High	Jan. 19, 2018 11:56:39	CS-SE-GB-CS	CSUSER	Unassigned	New
High	Jan. 19, 2018 11:49:44	CS-SE-GB-CS	CSUSER	Unassigned	New
High	Jan. 19, 2018 11:49:44	CS-SE-GB-CS	CSUSER	Unassigned	New
High	Jan. 19, 2018 11:47:43	CS-SE-GB-CS	CSUSER	Unassigned	New
High	Jan. 19, 2018 11:38:39	CS-SE-GB-CS	CSUSER	Unassigned	New

Executive dashboard



4.1.1.18 The software shall provide time stamping of all collected data and events based on a single time standard (e.g., coordinated universal time).

- By default, the Falcon UI displays times in the UI in local browser time for all detections and other components that use a time (with the exception of Event Search data, which uses UTC).

- Users have the option to choose which time zone they want to use for detection information. In addition, users can choose the desired date/time format.

4.1.1.19 The software shall have the ability to pull locally stored data from specified endpoints in near real time to support high priority hunt and forensic operations.

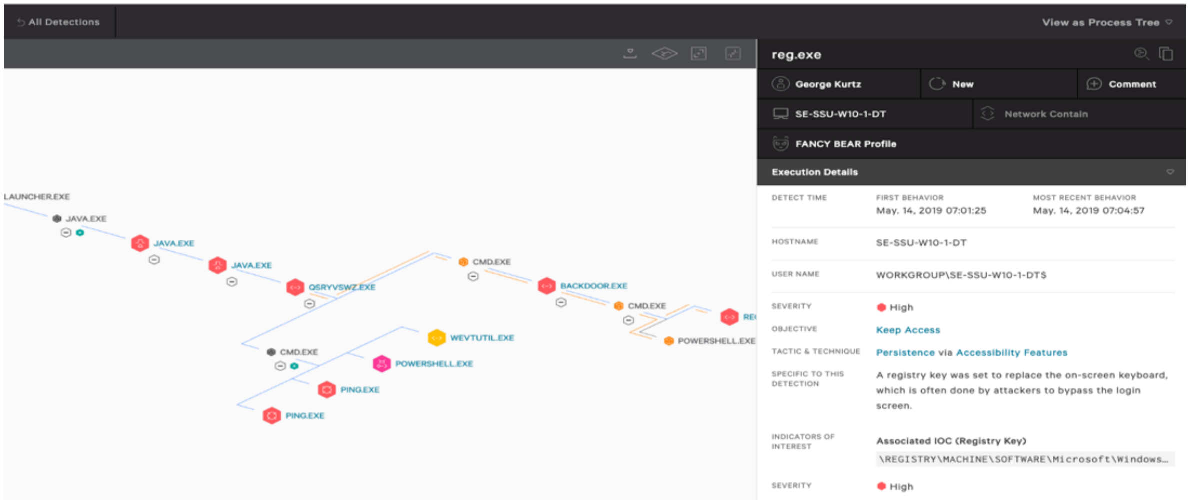
- Use real time response to run commands on a Windows host directly from the Falcon console. Real time response gives you more sophisticated incident response options than simply network containing a host, and you can connect to an online host immediately from any location.
- You can use real time response to perform many common response and remediation tasks, including:
    - Navigate the file system, upload or delete files, and perform many file system operations
    - List running processes and kill processes
    - Retrieve memory dumps, event logs, or any other files
    - Show network connections
    - Query, create, or modify registry keys
    - Remotely restart or shut down a host
    - Manage and run your own custom scripts or executables

4.1.1.20 The software shall provide automated analysis and visualization of an attack; including production of an event timeline and initial assessment of severity/impact

- CrowdStrike Falcon Platform UI presents in real-time detections/preventions in a simple to understand graphically rich format, which means you don't have to dig around the console to piece together different events involved in an attack. Our process timeline shows an entire attack in sequence with activity before the attack occurred and after it occurred. We also offer an interactive process visualization that allows you to pivot on different activity involved in an attack. Analysts can drill down into hosts, processes, and down to file reads by a process. All real-time event data is centralized in the cloud and available for reporting and analysis. The platform has as well the ability for reporting, with various dashboards available. Email notification and integration with SIEM can be used as well as a vehicle to consume alerts.

- Mapping alerts to the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&Ck) Framework allows you to understand even the most complex detections at a glance, shortening the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.

Process Tree



reg.exe

SE-SSU-W10-1-DT

DETECT TIME

FIRST BEHAVIOR May. 14, 2019 07:01:25

MOST RECENT BEHAVIOR May. 14, 2019 07:04:57

HOSTNAME SE-SSU-W10-1-DT

USER NAME WORKGROUP\SE-SSU-W10-1-DT$

SEVERITY High

OBJECTIVE Keep Access

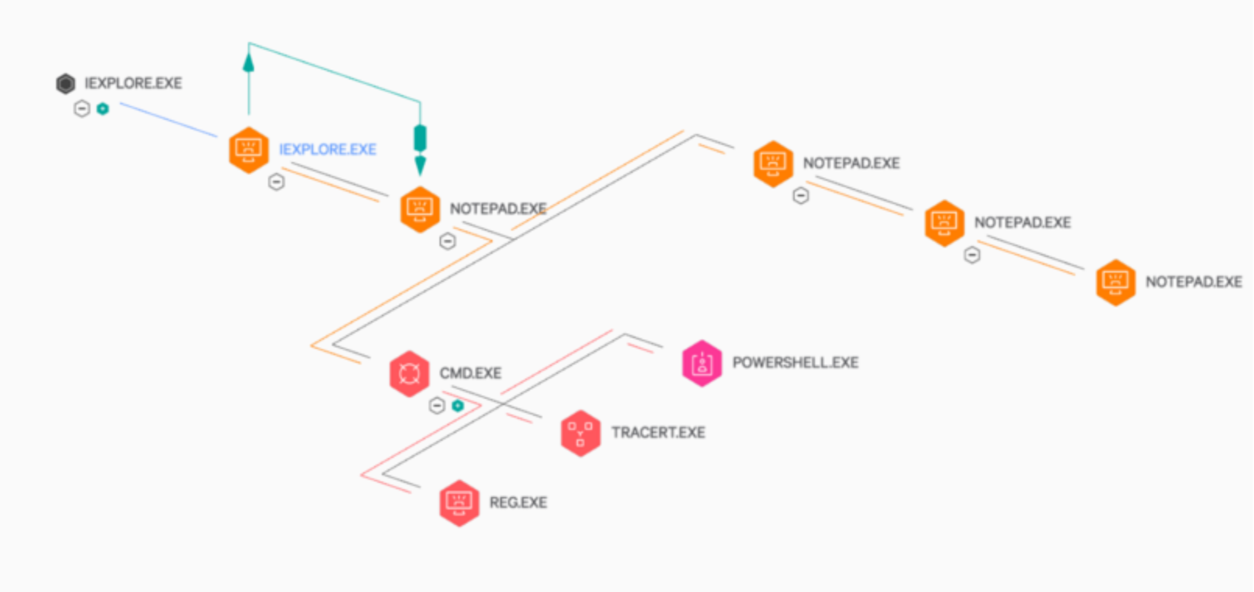
TACTIC & TECHNIQUE Persistence via Accessibility Features

SPECIFIC TO THIS DETECTION A registry key was set to replace the on-screen keyboard, which is often done by attackers to bypass the login screen.

INDICATORS OF INTEREST Associated IOC (Registry Key)

```
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows…
```

SEVERITY High



4.1.2 Technical Details

4.1.2.1 The Vendor must provide the minimum supported platforms including: Windows operating system, Linux operating system, and all virtual environments including but not limited to VMWare, Azure, and Hyper-V.

- 64-bit server OSes:
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Storage Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2 SP1
- 64-bit desktop OSes:
  - Windows 10 October 2018 Update, also named Redstone 5 or v1809
  - Windows 10 April 2018 Update, also named Redstone 4 or v1803
  - Windows 10 Fall Creators Update, also named Redstone 3 or v1709
  - Windows 10 Creators Update, also named Redstone 2 or v1703
  - Windows 10 Anniversary Update, also named Redstone 1 or v1607
  - Windows 10
  - Windows 8.1
  - Windows 7 SP1
  - Windows 7 Embedded
- 32-bit desktop OSes:
  - Windows 7 SP1
  - Windows 7 Embedded POSReady

Mac:

- macOS Mojave 10.14 and later *(sensor 4.13.7501 and later)*
- macOS High Sierra 10.13 and later *(sensor 3.6.5703 and later)*

  - macOS Sierra 10.12 and later

Linux:

We support x86_64 versions of these Linux server OSes.

- Amazon Linux 2
- Amazon Linux AMI
  - 2018.03
  - 2017.09
  - 2017.03
- CentOS
  - 7.1 – 7.6
  - 6.7 – 6.10
  - 8.0
- Oracle Linux
  - Oracle Linux 6 - UEK 3, 4
  - Oracle Linux 7 - UEK 3, 4, 5
  - Red Hat Compatible Kernel (supported RHCK kernels are the same as RHEL)

- Red Hat Enterprise Linux (RHEL)
  - 7.1-7.6
  - 6.7-6.10
  - 8.0
- SUSE Linux Enterprise
  - 15
  - 12.1 – 12.4
  - 11.4 (you must also install OpenSSL version 1.0.1e or greater)
- Ubuntu
  - 18-AWS
  - 18.04 LTS
  - 16-AWS
  - 16.04 LTS
  - 14.04 LTS

Docker is supported on RHEL 7, Ubuntu 14.04 and Ubuntu 16.04 with Falcon sensor for Linux 4.8.5305 and later. Docker is supported on CentOS 7 with Falcon sensor for Linux 4.11.5605 and later. Docker is supported on SLES 12 SP3 and Amazon Linux 2018.03 with Falcon sensor for Linux 4.15.6003 and later. No other operating systems or containers are currently supported.

Virtual Machines:
Falcon Endpoint Protection agent can be deployed without issue on VMware for each guest OS for Windows, MAC, and Linux.

Cloud protection:
Falcon Endpoint Protection agent can run on hosts in the cloud (AWS, Azure, etc..) some of our client take advantage of cloud technology to route network Traffic directly from the cloud to CrowdStrike cloud, equally use EC2 scripts and S3 buckets or similar technologies to rapidly deploy CrowdStrike Falcon Endpoint Protection agent.

- **OS Support:** The CrowdStrike Falcon app is supported for iOS and Android:
    - iOS 11 and later
    - Android 7.0 and later
- **MDM:** iOS - unsupervised devices require one of the following MDMs:
- Airwatch/VMware Workspace One
- MobileIron
- Microsoft Intune

4.1.2.2 The software shall not impair authorized system operations nor shall it degrade managed system performance in any way, which may adversely impact a system's primary business/mission functions. The following authorize system operations include but not limited to:

4.1.2.2.1 Patching, Scanning, Business software usage,

Falcon Discover module, uses the power of the cloud by leveraging already collected forensic meta data from endpoints to expose clients to IT Hygiene data to address the following

- Asset Discovery: See who is on your network at all times — The real-time system inventory gives you a view of all managed and unmanaged devices in the environment in a simple dashboard with drill-down options.

- Application Usage: Find out what applications your users are running. The real-time application inventory provides a view of all applications running in the environment via a simple dashboard with drill-down options. You can see what apps are currently running on which hosts without impacting the endpoint. You can also determine when the application was originally launched and pivot to other endpoints running the same app to gain more context, finding usage per application or by host.

- Privileged Account Usage: See where and how user accounts are being accessed across your environment. Account monitoring provides visibility into the use of administrator credentials and password resets across the enterprise. Falcon Discover provides insight into logon trends (activities/duration) where credentials are being used, and password update information.

- Strengthen your security posture proactively — Falcon Discover allows you to identify what is being utilized so you can ensure your best possible readiness to face attacks. By reporting unauthorized systems and applications in your environment, Falcon Discover enables you to improve your security posture by addressing security issues ahead of attacks.

- Detect unwanted and vulnerable applications — Detect whether unpatched or vulnerable applications are being used, so you can patch them before an attacker can take advantage.

4.1.2.2.2 The following Information Assurance Tools/Initiatives include but not limited to:

4.1.2.2.2.1 Secure host baseline, and assured compliance assessment software.

Falcon Discover™, a security hygiene solution that allows you to identify unauthorized systems and applications in real time across your environment, and remediate issues quickly to improve your overall security posture.

- APPLICATION VISIBILITY. See what apps are CURRENTLY running on which hosts – without impacting your endpoints. Determine when each application was originally launched, and pivot to other endpoints currently running the same app to gain more context. Find usage per application or by host.

- CREDENTIAL USE. Gain visibility into the use of administrator credentials across your enterprise and spot if they are being used inappropriately or out of context.
- IDENTIFY ROGUE SYSTEMS. Eliminate unprotected and unmanaged systems — a weak link that can create a bridge for adversaries to penetrate your network. Identify rogue systems to assess and remediate that vulnerability.
- REDUCE LICENSING COSTS. Real-time application inventory helps eliminate costly licensing fees by potentially identifying unused applications while satisfying your organization's operational needs.

4.1.2.3 The software shall allow for patching and update of containerized applications through a means of automated verification (e.g., integration with automated patch management infrastructure/processes).

- The Falcon Sensor updated is automated through CrowdStrike. Updating a sensor takes no effort on the part of the users. While it is recommended that the sensor is updated to take advantage of the extra feature enhancements and improved protection and detection capabilities, we recognize that some customers would like to control this aspect. Creating release groups allows customers this level of granularity and control over their environment.

4.1.2.4 All software components shall have the ability to be automatically deployed and configured based on predefined configurations.

- Deployment supported via SCCM, JAMF or any other 3rd party software distribution tool.
- The sensor is extremely lightweight and installs in under 30 seconds. There is no active disk scanning on the endpoint so there is no user impact. It consumes less than 20MB of memory, utilizes less than 1 % of CPU overhead, and takes approximately 40MB of space on disk with 2-10 MB of bandwidth usage over 24 hours.
- The Falcon sensor allows you to set a password during installation. Once a password has been set on a host, you must provide that password to unload, uninstall, repair, or manually upgrade the Falcon sensor. This feature makes the sensor more tamper resistant. CrowdStrike is a kernel driver, with a password protected install feature.

- **Cloud Managed Uninstall Protection**
  - We now offer more control over sensor uninstallation permissions using sensor update policies. Sensor update policies now include an Uninstall and maintenance protection setting that prevents the sensor from being uninstalled from hosts in that policy when enabled.
  - If the sensor can't connect to the cloud or if time-sensitive changes are required, admins can reveal single-use, sensor-specific maintenance tokens from the Host Management page that override the Uninstall and maintenance protection setting.

- CrowdStrike holds patents specific to installing with no reboot or restart required for full functionality

4.1.2.5 The software shall securely store and transmit data in a manner that ensures the confidentiality, integrity, availability, and source authenticity of the data.

- CrowdStrike uses an SSL/TLS-encrypted tunnel to send data between the sensor and the cloud.

- Additionally, CrowdStrike uses certificate pinning on the sensor side. This means that a sensor will only communicate with cloud endpoints that have a known certificate. CrowdStrike also provides you the ability to whitelist our cloud endpoints in your firewalls to ensure that your Falcon sensors only communicate with CrowdStrike.

- Next, every customer is assigned a unique customer ID. Because CrowdStrike tags customer data with a unique customer ID, any query or exchange of data will be limited to the scope of a specific customer ID, which further secures data.

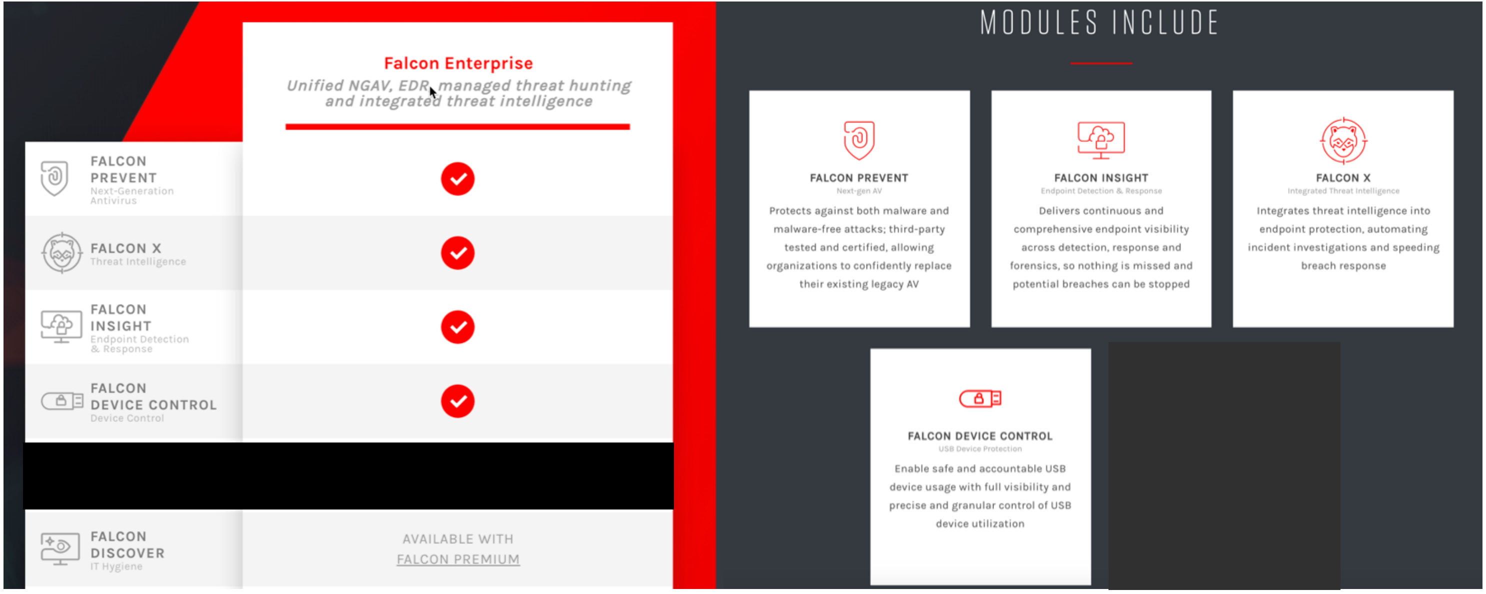
- Once data is in the CrowdStrike cloud, all data, including backups, are encrypted with industry-standard AES256 encryption.

- CrowdStrike also limits employee access to customer data to individuals with a business need. This includes Customer Support. Moreover, direct access to underlying systems is limited only to engineers with a business need. Access is protected by encrypted VPN and multi-factor authentication.

4.1.2.6 The software shall encrypt all data in transit or data at rest with Federal Information Processing Standards (FIPS) 140-2 compliant cryptographic modules.

- CrowdStrike Falcon can be used to address the requirements of the HIPAA security, including specific privacy rules for organizations implementing HIPAA (Health Insurance Portability and
- Accountability Act). CrowdStrike Falcon has been independently validated to assist healthcare organizations achieve compliance with HIPAA. CrowdStrike Falcon was identified as addressing eight separate key HIPAA technical requirements:
- A report was produced by Coalfire, a PCI Qualified Security Assessor (QSA) and outlines CrowdStrike Falcon's functionality with respect to PCI DSS v3.2. CrowdStrike Falcon meets all elements of requirement No. 5: "Protect all systems against malware and regularly update antivirus software or programs." In addition, CrowdStrike Falcon provides assistance with meeting four additional PCI requirements.
- Once data is in the CrowdStrike cloud, all data, including backups, are encrypted with industry-standard AES256 encryption.

Proposed Bundle:



	Falcon Enterprise *Unified NGAV, EDR, managed threat hunting and integrated threat intelligence*
FALCON PREVENT Next-Generation Antivirus	✓
FALCON X Threat Intelligence	✓
FALCON INSIGHT Endpoint Detection & Response	✓
FALCON DEVICE CONTROL Device Control	✓
[redacted]	
FALCON DISCOVER IT Hygiene	AVAILABLE WITH FALCON PREMIUM

MODULES INCLUDE

FALCON PREVENT
Next-gen AV
Protects against both malware and malware-free attacks; third-party tested and certified, allowing organizations to confidently replace their existing legacy AV

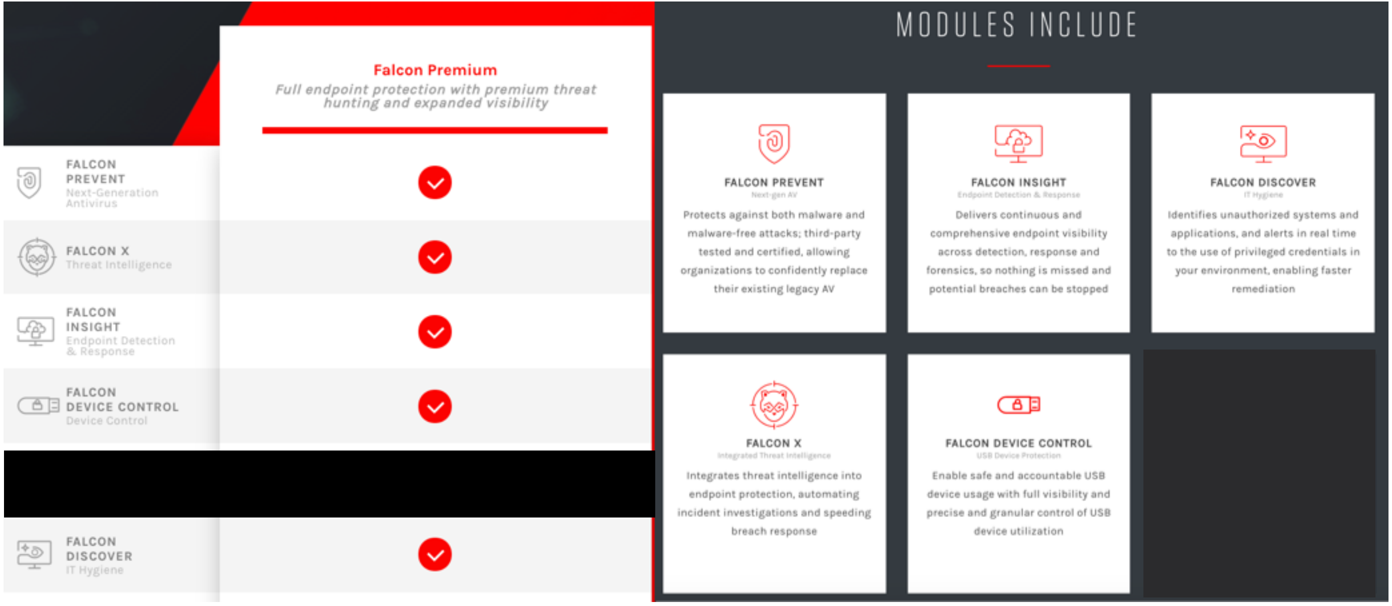
FALCON INSIGHT
Endpoint Detection & Response
Delivers continuous and comprehensive endpoint visibility across detection, response and forensics, so nothing is missed and potential breaches can be stopped

FALCON X
Integrated Threat Intelligence
Integrates threat intelligence into endpoint protection, automating incident investigations and speeding breach response

FALCON DEVICE CONTROL
USB Device Protection
Enable safe and accountable USB device usage with full visibility and precise and granular control of USB device utilization

[redacted]

Optional Bundle:



	Falcon Premium *Full endpoint protection with premium threat hunting and expanded visibility*
FALCON PREVENT Next-Generation Antivirus	✓
FALCON X Threat Intelligence	✓
FALCON INSIGHT Endpoint Detection & Response	✓
FALCON DEVICE CONTROL Device Control	✓
[redacted]	
FALCON DISCOVER IT Hygiene	✓

MODULES INCLUDE

FALCON PREVENT
Next-gen AV
Protects against both malware and malware-free attacks; third-party tested and certified, allowing organizations to confidently replace their existing legacy AV

FALCON INSIGHT
Endpoint Detection & Response
Delivers continuous and comprehensive endpoint visibility across detection, response and forensics, so nothing is missed and potential breaches can be stopped

FALCON DISCOVER
IT Hygiene
Identifies unauthorized systems and applications, and alerts in real time to the use of privileged credentials in your environment, enabling faster remediation

FALCON X
Integrated Threat Intelligence
Integrates threat intelligence into endpoint protection, automating incident investigations and speeding breach response

FALCON DEVICE CONTROL
USB Device Protection
Enable safe and accountable USB device usage with full visibility and precise and granular control of USB device utilization

4.1.3 Optional Renewals

4.1.3.1 Vendor should include, as part of its bid, pricing for optional renewal years 2, 3, and 4. These optional renewal years will be agreed upon by both parties and initiated by the Agency via Change Order. The contract will be awarded on the initial year's cost only.

5. CONTRACT AWARD:

5.1 Contract Award: The Contract is intended to provide Agency with a purchase price for the Contract Services. The Contract shall be awarded to the Vendor that provides the Contract Services meeting the required specifications for the lowest overall total cost as shown on the Pricing Pages.

Contract will be evaluated on all lines but only awarded on first year.

Renewal options for years 2, 3, and 4 will be initiated by the Agency, agreed to by the Vendor and processed by the West Virginia Purchasing Division as Change Orders for subsequent years.

Vendor should provide with their bid a copy of any and all Software Terms and Conditions or licenses that the State of West Virginia or the Agency will have to agree to or accept as a part of this solicitation. This information will be required before contract is issued.

Vendor should include a copy of any Maintenance Terms and Conditions or Licenses that the State of West Virginia or the Agency will be required to agree to and accept as a part of this solicitation. This information will be required before contract is issued.

5.2 Pricing Page: Vendor should complete the Pricing Page, Exhibit "A", by inserting the unit cost of the items listed; extended cost; and an overall total to reflect Total Cost of the listed items. See pricing page example. Vendor should complete the Pricing Page in full as failure to complete the Pricing Page in its entirety may result in Vendor's bid being disqualified.

Pricing Page Example

Estimated Quantity x Unit Cost = Extended Cost

The Pricing Pages contain a list of the Contract Items and estimated purchase volume. The estimated purchase volume for each item represents the approximate volume of anticipated purchases only. No future use of the Contract or any individual item is guaranteed or implied.

The Vendor can request an electronic copy of the Pricing Pages for bid purposes by sending an email request to the following address: Jessica.S.Chambers @wv.gov.

6. **PERFORMANCE:** Vendor and Agency shall agree upon a schedule for performance of Contract Services and Contract Services Deliverables, unless such a schedule is already included herein by Agency. In the event that this Contract is designated as an open-end contract, Vendor shall perform in accordance with the release orders that may be issued against this Contract.

7. **PAYMENT:** Agency shall pay flat fee for the unit cost, as shown on the Pricing Pages, for all Contract Services performed and accepted under this Contract. Vendor shall accept payment in accordance with the payment procedures of the State of West Virginia.

8. **TRAVEL:** Vendor shall be responsible for all mileage and travel costs, including travel time, associated with performance of this Contract. Any anticipated mileage or travel costs may be included in the flat fee or hourly rate listed on Vendor's bid, but such costs will not be paid by the Agency separately.

9. **FACILITIES ACCESS:** Performance of Contract Services may require access cards and/or keys to gain entrance to Agency's facilities. In the event that access cards and/or keys are required:

9.1 Vendor must identify principal service personnel which will be issued access cards and/or keys to perform service.
9.2 Vendor will be responsible for controlling cards and keys and will pay replacement fee, if the cards or keys become lost orstolen.
9.3 Vendor shall notify Agency immediately of any lost, stolen, or missing card or key.
9.4 Anyone performing under this Contract will be subject to Agency's security protocol and procedures.
9.5 Vendor shall inform all staff of Agency's security protocol and procedures.

10. **VENDOR DEFAULT:**

10.1 The following shall be considered a vendor default under this Contract.

10.1.1 Failure to perform Contract Services in accordance with the requirements contained herein.

10.1.2 Failure to comply with other specifications and requirements contained herein.

10.1.3 Failure to comply with any laws, rules, and ordinances applicable to the Contract Services provided under this Contract.

10.1.4 Failure to remedy deficient performance upon request.

10.2 The following remedies shall be available to Agency upon default.

10.2.1 Immediate cancellation of the Contract.

10.2.2 Immediate cancellation of one or more release orders issued under this Contract.

10.2.3 Any other remedies available in law or equity.

11. MISCELLANEOUS:

11.1 **Contract Manager:** During its performance of this Contract, Vendor must designate and maintain a primary contract manager responsible for overseeing Vendor's responsibilities under this Contract. The Contract manager must be available during normal business hours to address any customer service or other issues related to this Contract. Vendor should list its Contract manager and his or her contact information below.

Contract Manager:	John Joaquin
Telephone Number:	301-302-1202
Fax Number:	N/A
Email Address:	jjoaqui@us.ibm.com

EXHIBIT A - Pricing Page
EndPoint Detection and Response Services - OT19125
Note to Vendors: The Pricing Page is locked with the exception of Unit Cost column.

Line Items	Description	Unit of Measure	Estimated Ouantitv	Unit Cost
4.1	**Contract Item: Endpoint Detection and Response Software for approximately 2,000 Endpoints**	**LS**	**I**	**$164,113.93**
4.1	**Optional Renewal Year 2 Maintenance: Contract Item: Endpoint Detection and Response Software**	**LS**	**I**	**$148,088.68**
4.1	**Optional Renewal Year 3 Maintenance: Contract Item: Endpoint Detection and Response Software**	**LS**	**I**	**$148,088.68**
4.1	**Optional Renewal Year 4 Maintenance: Contract Item: Endpoint Detection and Response Software**	**LS**	**I**	**$148,088.68**
			Total Overall Cost	**$608,379.97**

Please note: This information is being captured for auditing purposes

Contract will be evaluated on all lines but only awarded on first year. Renewal options for years 2, 3, and 4 will be initiated by the Agency, agreed to by the Vendor and processed by the WV Purchasing Division as Change Orders for subsequent years.

Vendor Signature:

Purchasing Division

PURCHASING AFFIDAVIT

CONSTRUCTION CONTRACTS: Under W. Va. Code § 5-22-1(i), the contracting public entity shall not award a construction contract to any bidder that is known to be in default on any monetary obligation owed to the state or a political subdivision of the state, including, but not limited to, obligations related to payroll taxes, property taxes, sales and use taxes, fire service fees, or other fines or fees.

ALL CONTRACTS: Under W. Va. Code §SA-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate, or (2) the debtor is in employer default.

EXCEPTION: The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

DEFINITIONS:

"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

"Employer default" means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repaymentagreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

"Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceed five percent of the total contract amount.

AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing *(W. Va. Code* §61-5-3) that: (1) for construction contracts, the vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.

WITNESS THE FOLLOWING SIGNATURE:

Vendor's Name: IBM Corporation

Authorized Signature: ________________________ Date: 7/30/2019

State of ________________

County of ______________, to-wit:

Taken, subscribed, and sworn to before me this_day of ________________, 20_.

My Commission expires ________________, 20_

AFFIX SEAL HERE **NOTARY PUBLIC _**

____

Appendix A

Pursuant to the instructions of this solicitation, International Business Machines Corporation ("IBM" or "Vendor") offers its clarifications and proposed modifications to the terms and conditions listed in **Request for Quotation 21 - Info Technology** (the "RFQ"), as set forth below. During negotiations with the State of West Virginia, IBM reserves the right to identify and negotiate terms and conditions in addition to those listed herein. IBM's proposal is expressly conditioned upon the negotiation of a mutually acceptable set of terms and conditions.

RFQ Provision	IBM's Proposed Alternative Language
36. INDEMNIFICATION: The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction , deliver y, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws.	***The below provision agreed to between the State of WV and IBM on 2/27/2017*.** **INDEMNIFICATION AND LIMITATION OF LIABILITY:** Vendor shall defend, indemnify, protect, save and hold harmless, to the extent Vendor is legally liable, Agency, its officers and employees from and against any and all claims or causes of action, damages or costs, including attorney's fees, for patent, copyright, trademark or trade secret infringement, and bodily injury or damage to real or tangible personal property, arising from the negligent or willful acts or omission of the Vendor, or its agents, employees, or subcontracts in the performance of this Agreement. Vendor shall not be liable for damage that arc the result of negligence or intentional wrong doing by the Agency or its employees. This clause shall not be construed to bar any legal remedies the Vendor may have with Agency's failure to fulfill its obligations pursuant to this Agreement. Agency agrees that the Vendor, its principals, members and employees shall not be liable to the Agency, unless otherwise stated in the applicable Addendum, for any actions, damages, claims, liabilities, costs, expenses, or losses in any way arising out of or relating to this Agreement or the Products provided or Services performed hereunder for an aggregate amount in excess of two times the value of the Products provided or Services performed under this Agreement. The foregoing limitation does not apply to patent, copyright, trademark or trade secret infringement claims for which Vendor must indemnify Agency under this Agreement, or to damages resulting from bodily injury caused by the Vendor's negligence. In no event shall the Vendor be liable for any indirect, special, punitive, or consequential damages arising out of this Agreement or the use of the Products or Services purchased by the Agency hereunder, loss of, or damage to, data, lost profits, business, revenue, goodwill, or anticipated savings even if the Vendor has been advised of the possibility of such damages. Both parties agree that this Agreement does not create any right or cause for any third party against the other except for third party claims that fit within the identification provision of this Agreement.

The adjacent provision proposed by IBM to be added >>>	**45. European General Data Protection Regulations.** The State agrees that no State personal data that is subject to European General Data Protection Regulations (GDPR) requirements will be provided to Vendor under this Contract. In the event of a change, the State will notify Vendor in writing and a Data Processing Addendum (DPA) agreed to between the parties will apply and supplements the Contract.

CROWDSTRIKE

CROWDSTRIKE SUPPORT OFFERINGS

Standard | Express | Essential | Elite

CrowdStrike offers support services to assist with deployment and ongoing use of our products to ensure your success in “stopping the breach.” The CrowdStrike Support organization is dedicated to resolving any issues quickly and effectively. CrowdStrike provides multiple levels of support so customers can choose the level that best fits their business requirements and ensures that you receive the most from your investment in CrowdStrike. CrowdStrike provides four levels of support:

Standard Support is bundled free with Falcon Host, and provides basic support services such as email communications to the CrowdStrike Support team, access to the support portal and basic troubleshooting and technical assistance.

Express Support is created for customers in mission critical environments with less that 2,500 endpoints who require that deployment and operational issues are resolved as quickly as possible.

Essential support provides everything included in Standard support, plus:

- Extended coverage and expediated response times
- Prioritized case handling
- More communications options
- Quartlery health checks and reports
- Knowledge transfer opportunities
- Direct access to CrowdStrike’s team of Technical Account Managers

Essential Support is designed to provide peace of mind for larger environments (2,500+ endpoints). From planning to deployment, to ongoing operations, our team of support professionals understand the importance of your mission and are committed to working with you to avoid problems and resolve issues as fast as possible.

This program is for Security and IT Operations organizations that are using CrowdStrike for EPP and NGAV. Companies that value proactive services to avoid issues and fast and predictable access to support will benefit from this service.

Essential support provides everything included in Express support, plus:

- Hands-on assistance with deployment
- Invitations to Beta Programs
- Periodic proactive calls and customized reports covering overall health of your implementation, new best practices, feature requests, whitelist tuning, case status, product training, etc.

Elite Support is the highest level of support provided by CrowdStrike. A dedicated technical account manager works closely with you as your trusted advisor.

This program is for Security and IT Operations organizations that are using CrowdStrike for EPP and NGAV and want to supplement their staff with expert technical help, and highly predictable response times.

Elite support builds on CrowdStrike Essential Support and adds a named TAM, and custom reports.

COMPARISON CHART	STANDARD	EXPRESS	ESSENTIAL	ELITE
Communication channels				
Standard Portal	√	√	√	√
Email	√	√	√	√
Enhanced Portal			√	√
Phone	P1 or P2 issues only	P1 or P2 issues only	P1 or P2 issues only	P1 or P2 issues only
Number of dedicated contacts	N/A	6	6	6
Standard Coverage				
Standard Response time	Next business day	4 business hours	4 business hours	4 business hours
Standard coverage time	M-F 9am-6pm local time	M-F 8am-6pm local time	M-F 8am-6pm local time	M-F 8am-6pm local time
Critical Issues Coverage				
Critical Issues Response Time	1 hour	1 hour	1 hour	1 hour
Critical Issues Coverage Time	24x7	24/7	24/7	24/7
Dedicated phone number		√	√	√
Dedicated email hotline		√	√	√
Dedicated portal		√	√	√
Case management				
Case handling	Standard	Prioritized	Prioritized	Prioritized
Escalation path/Case oversight		√	√	√
On-going resolution		√	√	√
Proactive support		√	√	√
Defect handling	√	√	√	√
Expedited defect handling		√	√	√
Feature request	√	√	√	√
Prioritized feature requests		√	√	√
Other				
Quick-start Session		√	√	√
Roadmap participation			√	√
Hands-on deployment assistance			√	√
Technical Account Managers		√	√	√
Account history		√	√	√
Quarterly check-in calls		√	√	√
Health Checks		√	√	Customized
Quarterly reports		√	√	√
Proactive Invitations to Beta Programs			√	√
Named TAM				√
Custom quarterly reports				√
Onsite visits (T&E required)				√

Descriptions

SUPPORT CARE

Response Time

Standard: The support engineer responds to technical issues within 1 business day of call or 1 business hour for critical issues.

Express, Essential: The Technical Account Manager (TAM) team responds to technical issues within 4 business hours of call or 1 business hour for critical issues.

Elite: The TAM team responds to technical issues within 4 business hours of call or 1 business hour for critical issues.

24X7 Critical Issue Support

Standard: For critical technical issues (P1 – Network down), the support team is available around the clock.

Express, Essential and Elite: For critical technical issues, the team will be available around the clock, escalating issues as appropriate for the quickest possible resolution. You will be given a dedicated number, dedicated email hotline and dedicated support portal for these cases.

Prioritized Case Handling

Express, Essential and Elite support cases take precedence over Standard cases at the same priority level.

Proactive Support

Essential and Elite: During periodic calls scheduled at your convenience, a member of the TAM team will provide Q&A or just-in-time training on topics of your choice, updates on the latest product features, and general platform health checks.

PRODUCT CARE

Defect Handling

Standard: When determined the issue could be caused by a defect in the product, a case will be opened on the customer's behalf and managed to resolution.

Express, Essential and Elite: When determined the issue could be caused by a defect in the product, customer's ticket will take precedence over others within the same priority level.

Feature Requests

Feature request to support will be queued up by Support with our product management team feature process.

ACCOUNT CARE

Technical Account Manager Team

Express, Essential and Elite: Direct access to the TAM team who will be your first line of support and liaison to Support and Product Management.

Account History/Documentation

The TAM team will keep your Account records – including Contacts, Environment, Activity, etc. up-to-date to ensure that all your interactions are as efficient and effective as possible.

Quarterly Check-in Calls

The TAM team will schedule quarterly check-in calls at your convenience to:

- Review issues, projects, and goals
- Address any new questions or concerns
- Discuss Best Practices
- Provide updates on new Features
- Provide Just-In-Time training on any topics of your choice
- Health Check

Health Check

The TAM team reviews notifications, usage data, endpoint data, etc. to ensure that the platform is being used as efficiently and effectively as possible. If necessary, we will recommend configuration changes or upgrades to optimize your deployment.

Quarterly Service Reports

You receive a formal report summarizing the action items, recommendations, and other outcomes of each of the quarterly calls.

LET'S DISCUSS YOUR NEEDS
Phone: 1-888-512-8906
Email: sales@crowdstrike.com
Web: http://www.crowdstrike.com/

CROWDSTRIKE

15440 Laguna Canyon Road
Suite 250, Irvine, California 92618