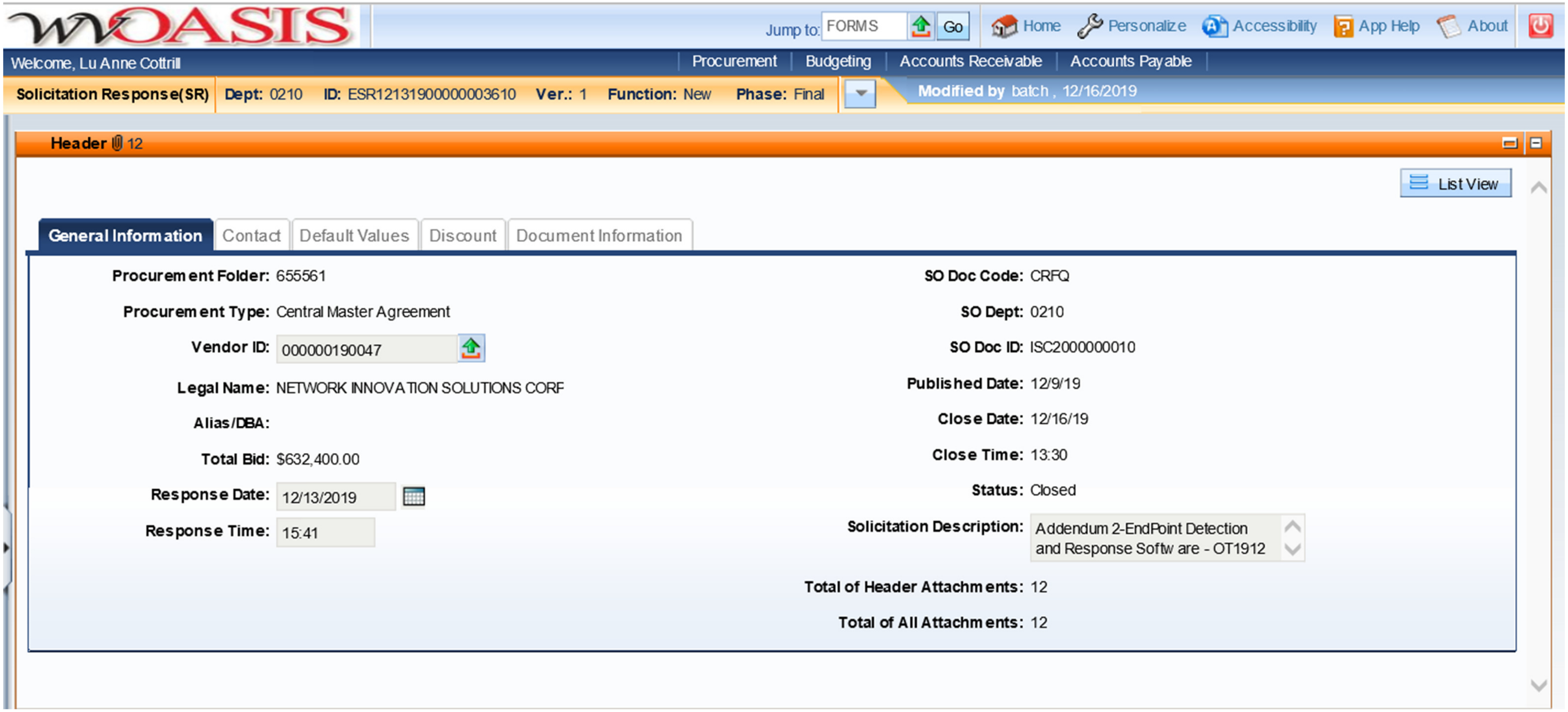
West Virginia
Purchasing Division

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

The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at *wvOASIS.gov*. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at *WVPurchasing.gov* with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.



Welcome, Lu Anne Cottrill

Solicitation Response(SR) **Dept:** 0210 **ID:** ESR12131900000003610 **Ver.:** 1 **Function:** New **Phase:** Final

Modified by batch , 12/16/2019

Header 12

Procurement Folder:	655561	**SO Doc Code:**	CRFQ
Procurement Type:	Central Master Agreement	**SO Dept:**	0210
Vendor ID:	000000190047	**SO Doc ID:**	ISC2000000010
Legal Name:	NETWORK INNOVATION SOLUTIONS CORF	**Published Date:**	12/9/19
Alias/DBA:		**Close Date:**	12/16/19
Total Bid:	$632,400.00	**Close Time:**	13:30
Response Date:	12/13/2019	**Status:**	Closed
Response Time:	15:41	**Solicitation Description:**	Addendum 2-EndPoint Detection and Response Softw are - OT1912
		Total of Header Attachments:	12
		Total of All Attachments:	12

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

State of West Virginia
Solicitation Response

Proc Folder : 655561

Solicitation Description : Addendum 2-EndPoint Detection and Response Software - OT1912

Proc Type : Central Master Agreement

Date issued	Solicitation Closes	Solicitation Response	Version
	2019-12-16 13:30:00	SR 0210 ESR12131900000003610	1

VENDOR

000000190047

NETWORK INNOVATION SOLUTIONS CORP

Solicitation Number: CRFQ 0210 ISC2000000010

Total Bid : $632,400.00 **Response Date:** 2019-12-13 **Response Time:** 15:41:58

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	CNTRCT ITEM: Containment Remediation Reporting & Monitoring	2000.00000	EA	$79.050000	$158,100.00

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Opt Renew Y2 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA	$79.050000	$158,100.00

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Opt Renew Y3 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA	$79.050000	$158,100.00

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Opt Renew Y4 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA	$79.050000	$158,100.00

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

STATE OF WEST VIRGINIA
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 §5A-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 repayment agreement 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: Network Innovation Solutions Corp

Authorized Signature: ______________________ Date: 12/13/2019

State of WV

County of Cabell, to-wit:

Taken, subscribed, and sworn to before me this 13 day of December, 2019.

My Commission expires May 21, 2022.

AFFIX SEAL HERE

NOTARY PUBLIC Jan Pelfrey

JAN M. PELFREY
Notary Public Official Seal
State of West Virginia
My Comm. Expires May 21, 2022
Metro Community FCU
PO Boix 5438 - 215 18th St Huntington WV 25703

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: ISC2000000010

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[X] Addendum No. 1

[X] Addendum No. 2

[ ] Addendum No. 3

[ ] Addendum No. 4

[ ] Addendum No. 5

[ ] Addendum No. 6

[ ] Addendum No. 7

[ ] Addendum No. 8

[ ] Addendum No. 9

[ ] Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Network Innovation Solutions Corp
Company

Authorized Signature

12/13/2019
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

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:	Robert Whitley
Telephone Number:	304-781-3410
Fax Number:	304-697-2183
Email Address:	rwhitley@gonis.us

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.

Robert Whitley CEO
(Name, Title)

Robert Whitley CEO
(Printed Name and Title)

821 4th Ave Huntington, WV 25703
(Address)

304-781-3410
(Phone Number) / (Fax Number)

rwhitley@gonis.us
(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.

Network Innovation Solutions Corp
(Company)

(Authorized Signature) (Representative Name, Title)

Robert Whitley CEO
(Printed Name and Title of Authorized Representative)

12/13/2019
(Date)

304-781-3410
(Phone Number) (Fax Number)

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: 655561

Doc Description: EndPoint Detection and Response Software - OT19125

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2019-11-21	2019-12-09 13:30:00	CRFQ 0210 ISC2000000010	1

BID RECEIVING LOCATION

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

VENDOR

Vendor Name, Address and Telephone Number: Network Innovation Solutions Corp
821 4th Ave Huntington, WV 25703
Phone: 304-781-3410

FOR INFORMATION CONTACT THE BUYER

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

Signature X FEIN # 46-1734617 DATE 12-13-19

All offers subject to 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 an open-end contract for an End Point Detection and Response Software to support 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. The open-end contract resulting from this solicitation will provide licensing for this platform, as needed per the terms and conditions and specifications as attached.

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	CNTRCT ITEM: Containment Remediation Reporting & Monitoring	2000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

4.1.1.2 The Vendor must provide a cloud-based software as a service solution that can be centrally managed by a West Virginia Office of Technology Administrator.

For further details see attached specifications.

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Opt Renew Y2 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

4.1.1.2 The Vendor must provide a cloud-based software as a service solution that can be centrally managed by a West Virginia Office of Technology Administrator.

For further details see attached specifications.

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
3	Opt Renew Y3 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

4.1.1.2 The Vendor must provide a cloud-based software as a service solution that can be centrally managed by a West Virginia Office of Technology Administrator.

For further details see attached specifications.

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
4	Opt Renew Y4 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

4.1.1.2 The Vendor must provide a cloud-based software as a service solution that can be centrally managed by a West Virginia Office of Technology Administrator.

For further details see attached specifications.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Technical Question Deadline 9:00 AM	2019-12-02

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 disqualification of 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 "shall." 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.

☑ 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 individual is permitted to represent more than one vendor at the pre-bid meeting. Any individual that does attempt to represent two or more vendors will be required to select one vendor to which the individual's attendance will be attributed. The vendors not selected will be deemed to have not attended the pre-bid meeting unless another individual attended on their behalf.

An attendance sheet provided at the pre-bid meeting shall serve as the official document verifying 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 disqualification of 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

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: 655561

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

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2019-12-06	2019-12-16 13:30:00	CRFQ 0210 ISC2000000010	2

BID RECEIVING LOCATION

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

VENDOR

Vendor Name, Address and Telephone Number:

Network Innovation Solutions Corp
821 4th Ave
Huntington WV 25703
Phone: 304-781-3410

FOR INFORMATION CONTACT THE BUYER

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

Signature X **FEIN #** 46-1734617 **DATE** 12-13-19

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

ADDITIONAL INFORMATION:

Addendum

Addendum No.01 is being issued to extend the bid opening date one wee to give the agency enough time to address all technical questions received.

New date and time is: 12/16/2019 at 1:30 PM (EST). .

****

The West Virginia Purchasing Division is soliciting bids on behalf of The WV Office of Technology to establish an open-end contract for an End Point Detection and Response Software to support 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. The open-end contract resulting from this solicitation will provide licensing for this platform, as needed per the terms and conditions and specifications as attached.

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	CNTRCT ITEM: Containment Remediation Reporting & Monitoring	2000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

4.1.1.2 The Vendor must provide a cloud-based software as a service solution that can be centrally managed by a West Virginia Office of Technology Administrator.

For further details see attached specifications.

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Opt Renew Y2 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

4.1.1.2 The Vendor must provide a cloud-based software as a service solution that can be centrally managed by a West Virginia Office of Technology Administrator.

For further details see attached specifications.

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
3	Opt Renew Y3 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

4.1.1.2 The Vendor must provide a cloud-based software as a service solution that can be centrally managed by a West Virginia Office of Technology Administrator.

For further details see attached specifications.

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
4	Opt Renew Y4 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

4.1.1.2 The Vendor must provide a cloud-based software as a service solution that can be centrally managed by a West Virginia Office of Technology Administrator.

For further details see attached specifications.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Technical Question Deadline 9:00 AM	2019-12-02

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

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: 655561

Doc Description: Addendum 2-EndPoint Detection and Response Software - OT1912

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2019-12-09	2019-12-16 13:30:00	CRFQ 0210 ISC2000000010	3

BID RECEIVING LOCATION

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

VENDOR

Vendor Name, Address and Telephone Number:

Network Innovation Solutions Corp
821 4th Ave Huntington, WV 25703
Phone: 304-781-3410

FOR INFORMATION CONTACT THE BUYER

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

Signature X **FEIN #** 46-1734617 **DATE** 12/13/2019

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

ADDITIONAL INFORMATION:

Addendum

Addendum No.02 is being issued to extend the bid opening date one wee to give the agency enough time to address all technical questions received.

New date and time is: 12/16/2019 at 1:30 PM (EST). .

****

The West Virginia Purchasing Division is soliciting bids on behalf of The WV Office of Technology to establish an open-end contract for an End Point Detection and Response Software to support 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. The open-end contract resulting from this solicitation will provide licensing for this platform, as needed 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
1	CNTRCT ITEM: Containment Remediation Reporting & Monitoring	2000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

4.1.1.2 The Vendor must provide a cloud-based software as a service solution that can be centrally managed by a West Virginia Office of Technology Administrator.

For further details see attached specifications.

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
2	Opt Renew Y2 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

4.1.1.2 The Vendor must provide a cloud-based software as a service solution that can be centrally managed by a West Virginia Office of Technology Administrator.

For further details see attached specifications.

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
3	Opt Renew Y3 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

4.1.1.2 The Vendor must provide a cloud-based software as a service solution that can be centrally managed by a West Virginia Office of Technology Administrator.

For further details see attached specifications.

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
4	Opt Renew Y4 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

4.1.1.2 The Vendor must provide a cloud-based software as a service solution that can be centrally managed by a West Virginia Office of Technology Administrator.

For further details see attached specifications.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Technical Question Deadline 9:00 AM	2019-12-02

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

WV-10
Approved / Revised
06/08/18

State of West Virginia
VENDOR PREFERENCE CERTIFICATE

Certification and application is hereby made for Preference in accordance with ***West Virginia Code***, §5A-3-37. (Does not apply to construction contracts). ***West Virginia Code***, §5A-3-37, provides an opportunity for qualifying vendors to request (at the time of bid) preference for their residency status. Such preference is an evaluation method only and will be applied only to the cost bid in accordance with the ***West Virginia Code***. This certificate for application is to be used to request such preference. The Purchasing Division will make the determination of the Vendor Preference, if applicable.

1. **Application is made for 2.5% vendor preference for the reason checked:**

☑ Bidder is an individual resident vendor and has resided continuously in West Virginia, or bidder is a partnership, association or corporation resident vendor and has maintained its headquarters or principal place of business continuously in West Virginia, for four (4) years immediately preceding the date of this certification; **or,**

□ Bidder is a resident vendor partnership, association, or corporation with at least eighty percent of ownership interest of bidder held by another entity that meets the applicable four year residency requirement; **or,**

□ Bidder is a nonresident vendor which has an affiliate or subsidiary which employs a minimum of one hundred state residents and which has maintained its headquarters or principal place of business within West Virginia continuously for the four (4) years immediately preceding the date of this certification; **or,**

2. **Application is made for 2.5% vendor preference for the reason checked:**

☑ Bidder is a resident vendor who certifies that, during the life of the contract, on average at least 75% of the employees working on the project being bid are residents of West Virginia who have resided in the state continuously for the two years immediately preceding submission of this bid; **or,**

3. **Application is made for 2.5% vendor preference for the reason checked:**

□ Bidder is a nonresident vendor that employs a minimum of one hundred state residents, or a nonresident vendor which has an affiliate or subsidiary which maintains its headquarters or principal place of business within West Virginia and employs a minimum of one hundred state residents, and for purposes of producing or distributing the commodities or completing the project which is the subject of the bidder's bid and continuously over the entire term of the project, on average at least seventy-five percent of the bidder's employees or the bidder's affiliate's or subsidiary's employees are residents of West Virginia who have resided in the state continuously for the two immediately preceding years and the vendor's bid; **or,**

4. **Application is made for 5% vendor preference for the reason checked:**

☑ Bidder meets either the requirement of both subdivisions (1) and (2) or subdivision (1) and (3) as stated above; **or,**

5. **Application is made for 3.5% vendor preference who is a veteran for the reason checked:**

□ Bidder is an individual resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard and has resided in West Virginia continuously for the four years immediately preceding the date on which the bid is submitted; **or,**

6. **Application is made for 3.5% vendor preference who is a veteran for the reason checked:**

□ Bidder is a resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard, if, for purposes of producing or distributing the commodities or completing the project which is the subject of the vendor's bid and continuously over the entire term of the project, on average at least seventy-five percent of the vendor's employees are residents of West Virginia who have resided in the state continuously for the two immediately preceding years.

7. **Application is made for preference as a non-resident small, women- and minority-owned business, in accordance with *West Virginia Code* §5A-3-59 and *West Virginia Code of State Rules.***

□ Bidder has been or expects to be approved prior to contract award by the Purchasing Division as a certified small, women- and minority-owned business.

8. **Application is made for reciprocal preference.**

□ Bidder is a West Virginia resident and is requesting reciprocal preference to the extent that it applies.

Bidder understands if the Secretary of Revenue determines that a Bidder receiving preference has failed to continue to meet the requirements for such preference, the Secretary may order the Director of Purchasing to: (a) rescind the contract or purchase order; or (b) assess a penalty against such Bidder in an amount not to exceed 5% of the bid amount and that such penalty will be paid to the contracting agency or deducted from any unpaid balance on the contract or purchase order.

By submission of this certificate, Bidder agrees to disclose any reasonably requested information to the Purchasing Division and authorizes the Department of Revenue to disclose to the Director of Purchasing appropriate information verifying that Bidder has paid the required business taxes, provided that such information does not contain the amounts of taxes paid nor any other information deemed by the Tax Commissioner to be confidential.

Bidder hereby certifies that this certificate is true and accurate in all respects; and that if a contract is issued to Bidder and if anything contained within this certificate changes during the term of the contract, Bidder will notify the Purchasing Division in writing immediately.

Bidder: Network Innovation Solutions Corp **Signed:**

Date: 12/13/2019 **Title:** CEO

**Check any combination of preference consideration(s) indicated above, which you are entitled to receive.*

RAPID7

Rapid7
120 Causeway Street
Suite 400
Boston, MA
02114
rapid7.com

Scope of Service

Rapid7 Managed Detection and Response (MDR)

Rapid7 Managed Detection and Response (MDR) enhances your ability to detect and respond to threats with hands-on 24/7/365 monitoring, threat hunting, and customized security guidance to stop nefarious activity and accelerate your security maturity.

Rapid7 MDR's outcome-driven focus advances your current security program by implementing our proven three-pronged approach to threat detection and response covering Technology, Security Expertise, and Process.

Technology

The Rapid7 MDR service leverages InsightIDR, our threat-focused Cloud SIEM, EDR, and UBA solution, to provide comprehensive protection against intruders in your internal network, devices, and cloud services. Additionally, the MDR SOC integrates event sources from your existing security infrastructure, granting the Rapid7 MDR team greater visibility into threats across your environment.

Rapid7 Cloud Technology Architecture and Capabilities

- **Insight cloud**: Responsible for all log management, data processing, enrichment, and storage of customer data. Each customer instance on the Insight cloud is isolated from other instances.
- **InsightIDR**: Rapid7's purpose-built cloud SIEM for incident detection and response combines real-time threat intelligence insights with a deep understanding of your environment and sophisticated behavior analytics to identify threats.
- **Rapid7 Threat Intelligence Engine**: Primary Rapid7-developed intelligence paired with additional third-party sources to enrich attack detection and response processes in near real time.

Customer-Deployed Software and Configuration

- **Insight Agent**: Powers the Insight cloud and allows Rapid7 analysts to collect data for identifying malicious activity on your endpoints for system-level visibility, real-time detection analysis, and endpoint investigation and hunting. We recommend deploying the Insight Agent on all endpoints, but require deployment to a minimum of 80% of licensed assets - defined as workstations, desktops, and servers - using your existing software management processes in order to deliver service. Rapid7 assigns deployment resources to work with you for the initial deployment of the Rapid7 MDR technology stack and ensure your event sources are configured for optimal service.
- **Insight Collector**: Responsible for receiving log data and agent data from your environment. All collected data is compressed and encrypted before being forwarded to the Insight cloud. The Collector also acts as a proxy for endpoint agents to reduce bandwidth constraints and increase endpoint scalability.

- **InsightIDR**: Rapid7 MDR provides full access to co-manage InsightIDR, including access to functionality such as investigations, log search, dashboard cards, and reporting. Your team can also establish custom alerts in InsightIDR; however, Rapid7 will be unable to act on these custom alerts beyond the monitoring that MDR typically covers. Additionally, your team should not modify or close out alerts within InsightIDR without contacting your Customer Advisor prior to closing out these alerts to ensure the Rapid7 MDR team maintains complete visibility.
- **Event Sources**: You are required to connect logs for four foundational event sources to the Insight Collector(s): Active Directory (for Windows assets), DHCP, DNS, and LDAP directory services (or equivalent as agreed upon with Rapid7). Rapid7 will validate connectivity and processing once deployment is complete. Rapid7 will also perform ongoing monitoring to evaluate the health of the technology stack and provide you with notifications when a failure or issue is identified.
- **Deception Technology (optional)**: Honeypots, honey users, honey credentials, and honey files designed to identify malicious behaviors using fake assets, users, credentials in memory, or files.

Linux & Mac limitations:

Rapid7's MDR service on endpoints (including workstations and servers) is delivered via the InsightAgent on devices running the Windows operating system. While the InsightAgent can be installed on Linux and Mac endpoints, the functions available for those operating systems through the agent are limited to actions that do not directly relate to threat detection and response. Therefore, Customer understands and accepts that the limited capabilities of the InsightAgent on Linux and Mac assets present a risk of coverage for those specific devices, and delivery of the service on endpoints is restricted to those that are running Windows.

Security Expertise

The Rapid7 MDR team consists of multiple functional groups working together to ensure you receive world-class service. We pride ourselves on becoming a true extension of your team through security expertise, attentive service, and dedicated resources to help advance your security posture.

MDR SOC Analysts:

Our MDR SOC teams of world-class analysts maintain 24/7/365 vigilance, from alert validation through in-depth forensics and analysis of your network and users. The SOC implements a three-tiered approach to provide optimal coverage for all alerts:

- **"Spotters"** look across all customers to validate and report on high-fidelity generated indicators from InsightIDR and the SOC’s proprietary tools. Spotters typically monitor for simple threat intelligence matches and Attacker Behavior Analytics (ABA).
- **"Hunters"** are assigned to individual customer clusters to ensure a deep understanding of each customer’s environment, as well as threat profiles specific to each industry. Hunters are responsible for validating and reporting on lower fidelity, technology-generated indicators like UBA and ABA alerts. They are also responsible for the monthly threat hunts.
- **"Responders"** support threat monitoring, hunting, and incident escalations by providing advanced remediation and mitigation recommendations gleaned from deep analysis of malware or APTs. Additionally, these individuals assist in developing customer-specific detections (e.g. specific

types of activities happening in the network) and work alongside our Threat Intelligence team to write new threat detections.

Customer Advisor

Your **Customer Advisor ("CA")** is your main point of contact for the Rapid7 MDR service. This person works with you as a strategic security partner—from initial technology deployment through incident remediation and ongoing security consultation—to shepherd your organization's security maturity. Throughout the service, your CA will frequently communicate with you to provide updates on service delivery, reporting, metrics, technology health, and ensure we are addressing your security goals. Customer Advisors are available during normal business hours, and a member of the CA team is on-call if malicious activity is detected outside of those hours.

Threat Intelligence Team

Rapid7's **Threat Intelligence team** supports the SOC and CAs with analysis and new detections. Our Rapid7 Threat Intelligence team of researchers identifies new attacker trends across the global threat landscape and uses these findings to create in-product detection mechanisms for new vulnerabilities, exploits, and attack campaigns.

Process

When a threat is detected, MDR SOC analysts will manually validate each detection by gathering context from your endpoints and logs to assess the severity. This approach enables quick identification and response to attacker activity with focused and prioritized containment, remediation, and mitigation recommendations.

Detection Methodologies

Rapid7 employs multiple detection methodologies to uncover malicious activity:

- **User Behavior Analytics (UBA)**: InsightIDR creates a baseline of normal user activity within your environment and generates investigative leads when there is a deviation.
- **Attacker Behavior Analytics (ABA)**: InsightIDR applies behavioral analytics to generate investigations, built from our experience and understanding of attacker tools, tactics, and methodologies.
- **Threat intelligence-based detection**: Rapid7 leverages proprietary threat intelligence derived from research, previous investigations, MDR monitoring findings, and third-party sources.
- **Threat hunts**: The MDR team performs monthly forensic analysis from Insight Agent data to identify unknown threats in your environment based on emerging trends in the threat landscape.
- **Human validation**: Rapid7 MDR analysts validate all events prior to reporting incidents to remove benign, unnecessary, or redundant alerts.

Threat Findings and Reporting

Rapid7 MDR service reports are delivered via the Rapid7 secure file transfer system located in your customer Services Portal. These include:

- **Compromise Assessment**: After deployment and prior to starting monitoring of your environment, Rapid7 MDR will ensure there is no malicious activity in your network or evidence of previous compromise(s). This report contains any detected active or historic compromises, potential avenues for future breaches, and prioritized remediation and mitigation recommendations.

- **Findings Reports**: Findings reports provide written analysis, criticality, raw details, remediation recommendations, suggested containment actions, and mitigation recommendations for each validated incident. Rapid7 will notify you of any malicious activity discovered during monitoring ("incident") via your preferred method within the timeframes outlined in the 'Response Times', and will generate an Initial Findings Report at the conclusion of each investigation.
- **Hunt Reports**: Hunt Reports contain metrics and findings related to endpoint forensic analysis activities performed by the MDR analysts. Our analysts leverage the Rapid7 Insight Agent to collect metadata from multiple locations on your endpoints to identify persistent malware, historical application execution, unusual processes and network communications, and per-system anomalies.
- **Monthly Service Reports**: Rapid7 will provide you with metrics and context surrounding analysis activities, technology health, and findings summaries for an at-a-glance overview of MDR activities.
- **Threat Intelligence Reports**: When Rapid7's Threat Intelligence infrastructure or third-party threat intelligence partners identify new vulnerabilities or detection patterns, the Rapid7 team will publish a highly targeted analysis of the threat to inform you of the findings.

Incident Escalations

In the event of a validated breach during the monitoring phase of your contract duration, Rapid7 will contact you with the option to exercise one of your **two (2) Incident Escalations each year** included in your MDR service per your contract, per the response times outlined below:

Escalation Activity	Time to Action
Time to begin escalation	Within 1 hour from initiation of incident escalation
Communications and updates	Daily updates, along with a daily debrief of the day's investigation results and progress. Substantial findings will be communicated regularly as they are discovered
Incident Escalation Report	Within 2 business days from completion of investigation

An Incident Escalation is a technical process handled by the Managed Services SOC. An incident escalation is triggered when a customer is compromised. All investigation activity is conducted remotely and is limited to examination of data obtainable by the InsightIDR agent and platform. Disk forensics are not included as part of an Incident Escalation (but available for Incident Response engagements which are outlined below).

Rapid7 MDR allocates SOC analysts for each Incident Escalation event. Activities performed during an Incident Escalation include:

- **Remote technical analysis and incident scoping**: The MDR team leverages Rapid7 cloud services and the Insight Agent to perform a remote incident investigation and scope attacker activity.

- **Daily reporting**: Rapid7 will provide a daily status report during the duration of the Incident Escalation detailing new findings and recommendations.
- **Final report**: At the conclusion of the Incident Escalation, Rapid7 will provide a final report detailing attacker activity supported by evidence with remediation and mitigation recommendations.

If your incident falls outside the scope of an Incident Escalation (i.e., pre-dating the start of your MDR monitoring phase, on-site help is needed, data collected outside of InsightIDR or the Insight Agent), or you wish to escalate more than two (2) incidents per year, Rapid7 will offer Incident Response services at a daily or weekly rate, as applicable per a separate Incident Response Services contract.

Response Times

The following response times are included as a part of the Rapid7 Managed Detection and Response service:

Investigation Validation: Based on the level of severity of an incident, the team will alert you per the response times outlined in the below table. It should be noted, criticality of an event is determined by the Rapid7 MDR SOC during the course of an investigation into an identified event. It is not possible to assign criticality before the scope of the event is determined. Validation is defined as the Rapid7 MDR SOC performing initial triage and investigation to determine with a high degree of confidence that the event is non-benign and requires a communication to the customer.

	Example behaviors	Target time to notification	Time to Findings Report
Critical Severity	An incident created via non-commodity malware deployed via spearphishing, social engineering, zero-day exploitation, or strategic web compromise, specifically targeted towards a target or organization	Within one (1) hour of validation; Ongoing communications as they become available, but at minimum, every 4 business hours. Significant findings will be communicated as they are identified.	Findings Report will be posted in the Services Portal within 24 hours upon completion of investigation
High Severity	An incident created using targeted off-the-shelf software backdoor deployed via spearphishing, social engineering, or strategic web compromise. Planned and targeted, but using common malware.	Within one (1) hour of validation; Ongoing communications as they become available, but at minimum, every 4 business hours. Significant findings will be communicated as they are identified.	Findings Report will be posted in the Services Portal within 24 hours upon completion of investigation
Medium Severity	An incident created using common threat malware, typically non specifically targeted, but rather opportunistic and automatic.	Within eight (8) hours of validation; Ongoing communications as they become available, but at minimum, every 8 business hours. Significant findings will be communicated as they are identified.	Findings Report will be posted in the Services Portal within 24 hours upon completion of investigation
Low Severity	An low-risk threat, not capable of remote code execution, credential	Within eight (8) hours of validation; Ongoing communications as they	Findings Report will be posted in the Services Portal within 24 hours

	harvesting, or data theft. (ex: Spam email delivering adware).	become available, but at minimum, every 8 business hours. Significant findings will occur as they are identified.	upon completion of investigation

Incident Escalation: Rapid7 MDR team will begin the Incident Escalation within one (1) hour once you have approved the escalation.

Technology Uptime: Rapid7 InsightIDR, which powers the MDR service, follows the same uptime availability reflected by Rapid7's overall Insight Platform Service Level Agreement.

Customer Advisor Response Times: Your Customer Advisor team is held to the following response times for notifications and responses to inquiries from your team:

- One (1) hour to proactively reach out to you for validated critical severity threats by phone to provide the relevant details quickly while the SOC team generates a threat report.
- Two (2) business hours to respond to an urgent request from your team at the discretion of the Customer Advisor team.
- One (1) business day to respond to a non-urgent request from your team at the discretion of the Customer Advisor team.

Requirements

Rapid7 Responsibilities and Requirements

- Monitor your environment in accordance with the detection methodologies outlined above and within the scope of the visibility provided by the technology stack
- Assist you with subject matter expertise to deploy the various required and optional technology stack components
- Provide a named Customer Advisor to accelerate your security maturity
- Conduct Incident Escalation investigations
- Provisioning and ongoing management of Rapid7 cloud services in the technology stack
- Deliver reports
- Notify you to any Customer Advisor or service delivery changes to your relationship with Rapid7 MDR

Customer Responsibilities and Requirements

- Ensure network connectivity between the log sources and the InsightIDR collector and from the InsightIDR collector to the Rapid7 Insight cloud
- Deploy Insight Agent to a minimum of 80% of licensed workstation, desktop, and server assets
- Designate a project manager to work with Rapid7
- Designate a primary point of contact and escalation path for reporting incidents
- Complete the Deployment Survey prior to starting the deployment
    - Deploy required and optional customer site technology stack components
    - Ensure key network, security, or other personnel are accessible as necessary for services

    - Provide Rapid7 with relevant documentation (i.e., policies, procedures, diagrams, flow charts, etc.) necessary for MDR service
    - Ensure availability of customer site deployed technology including Insight Collector, log sources, optional deception technology, and the Insight Agent; as well as their ability to report to Rapid7 infrastructure
    - Update the Rapid7 Insight Agent (if auto-updating is not enabled.) The Rapid7 MDR service supports the current version of the Agent and up to two previous versions as signified by a change in the ones (x), tenths (y) or hundredths (z) of a version (x.y.z)
- Allocate and configure space in one or more virtual computing platforms, and install Insight Collector(s) as required
    - Identify and configure log sources to send to the InsightIDR service
        - You may optionally connect any User Attribution or Security Data from InsightIDR Supported Event Sources.
        - Additional sources will be available for log search and reporting, but are not guaranteed to be included in the detection and alerting process
- Notify Rapid7 to any personnel, technology, event source, or point of contact changes or modifications

_________________________________ Customer Name

_________________________________ Title

_________________________________ Company

_________________________________ Signature

_________________________________ Date

Terms and Conditions

This Services Brief is governed by Rapid7’s standard Master Services Agreement available at https://www.rapid7.com/legal/terms/ unless the parties have a fully executed Master Services Agreement which supersedes such standard terms. Any changes in materials or scope of work as defined in this document must be agreed upon in writing by you and Rapid7. Customer deployed software and related services are governed by the Rapid7 Terms of Service available at https://www.rapid7.com/legal/terms.

NIS
NETWORK INNOVATION
SOLUTIONS

Solicitation ISC2000000010

West Virginia
OFFICE OF TECHNOLOGY

Delivered on:

12/13/2019

Submitted by:

Network Innovation Solutions

Managed Detection and Response (MDR)

Solicitation ISC2000000010

Department of Administration
Office of Technology
1900 Kanawha BLVD E BLDG 5 10th Floor
Charleston, WV 25305

On behalf of Network Innovation Solutions, it is a privilege to submit the following response to the State of West Virginia Office of Technology for solicitation ISC2000000010. For more than six years Network Innovation Solutions has worked collaboratively across public and private sectors to ensure affordable IT products and services, creating a better business environment.

We have provided the WVOT with a price proposal for solicitation ISC2000000010 using Rapid 7 Managed Detection and Response Service. This meets all specifications listed within the solicitation. We have attached all the documentation with the bid.

Please accept this response and commitment on this Project to WVOT. If you should have any questions, feel free to contact me by email rwhitley@gonis.us or by phone at 304-781-3410.

Sincerely,

Robert Whitley

Chief Executive Officer

Our Team Dedicated to WV Office of Technology

Robert Whitley - CEO

rwhitley@gonis.us

Jim Thomas - CTO

jthomas@gonis.us

Rapid7 Managed Detection and Response (MDR)

Below you will find a collection of sample Rapid7 MDR service deliverables (reports). These include:

Compromise Assessment View Report

Immediately after deployment and prior to starting monitoring of your environment, Rapid7 MDR will ensure there is no malicious activity in your network or evidence of previous compromise(s). This report contains any detected active or historic compromises, potential avenues for future breaches, and prioritized remediation and mitigation recommendations.

Findings Reports View Report

Findings reports provide written analysis, criticality, raw details, remediation recommendations, suggested containment actions, and mitigation recommendations for each validated incident. Rapid7 will notify you of any malicious activity discovered during monitoring ("incident") via your preferred method within one (1) hour from the initial validation and will generate an Initial Findings Report at the conclusion of each investigation.

Hunt Reports View Report

Hunt Reports contain metrics and findings related to endpoint forensic analysis activities performed by the MDR analysts. Our analysts leverage the Rapid7 Insight Agent to collect metadata from multiple locations on your endpoints to identify persistent malware, historical application execution, unusual processes and network communications, and per-system anomalies.

Monthly Service Reports View Report

Rapid7 will provide you with monthly metrics and context surrounding analysis activities, technology health, and findings summaries for an at-a-glance overview of MDR activities.

Threat Intelligence Reports (Monthly) View Report

Rapid7's Threat Intelligence team assembles monthly reports for all Managed Services customers to alert your team of changes we see in the threat landscape, including evidence from Project Heisenberg and Project Sonar, with highly targeted analysis of each threat.

Threat Intelligence Reports (Ad-hoc) View Report

When Rapid7's Threat Intelligence infrastructure or third-party threat intelligence partners identify new vulnerabilities or detection patterns that pose critical risk to our customers, the Rapid7 team will publish an ad-hoc, highly targeted analysis of the threat to inform you of the findings.

RAPID7

SERVICE OVERVIEW

Managed Detection and Response

Stop nefarious activity and accelerate your security maturity with hands-on, 24/7/365 monitoring, threat hunting, and tailored security guidance.

TABLE OF CONTENTS

Introduction to MDR

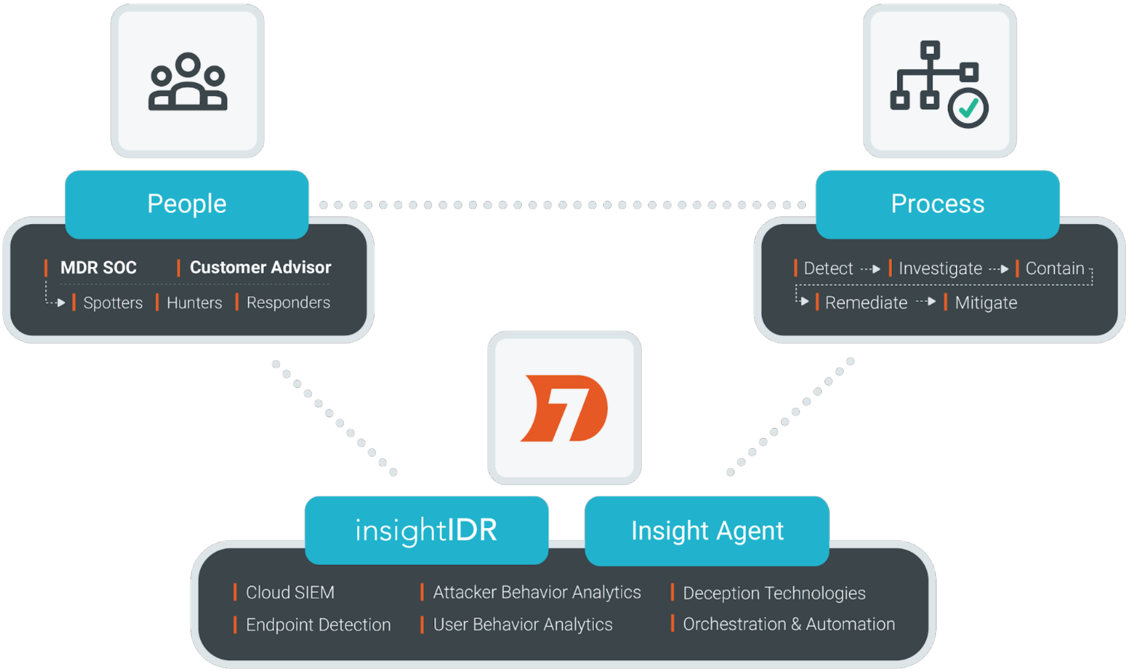
Rapid7’s Managed Detection and Response (MDR) service offers a combination of expertise and technology to detect dynamic threats quickly across your entire ecosystem. Our MDR service provides hands-on, 24x7x365 threat monitoring and hunting customized to your business profile, powered by Rapid7’s purpose-built technology stack. This includes the Rapid7 Insight cloud and Threat Intelligence infrastructure, in addition to our Security Operations Center (SOC) experts who work to help you remediate risks quickly, so you can accelerate your security maturity.

This document outlines Rapid7’s MDR service.

Rapid7's MDR Approach

At its core, Rapid7's MDR service is a strategic partnership that allows your business to strengthen your security program maturity as it relates to threat detection and response. Rapid7 MDR extends your existing team to detect, investigate, report, and recommend response actions to threats in your network. We do this through 24x7x365 monitoring by a team of security experts, leveraging proven cloud SIEM technology, cutting-edge endpoint technology, and world-leading threat intelligence to stay ahead of attackers. When engaging with this service, you'll gain a true security partner who can provide the mentorship and guidance necessary to simplify the complexities of cybersecurity and help you securely advance your business.

Our focus on advancing your current maturity level in incident detection and response layers our industry experts, workflow processes, and technology to implement our three-pronged approach:


People
MDR SOC | Customer Advisor
Spotters | Hunters | Responders

Process
Detect → Investigate → Contain
Remediate → Mitigate

insightIDR | Insight Agent
Cloud SIEM | Attacker Behavior Analytics | Deception Technologies
Endpoint Detection | User Behavior Analytics | Orchestration & Automation

People

Your environment is monitored 24x7x365 by world-class SOC analysts, each with years of experience building detection and response programs, and hunting for and validating threats.

SOC Analysts leverage specialized toolsets, malware analysis, tradecraft, and forward-looking collaboration with Rapid7's Threat Intelligence researchers to make detection and remediation of threats possible. The Threat Intelligence researchers are constantly monitoring our MDR customer environments, as well as the global threat landscape to enhance the MDR team's detection methodologies.

These teams are augmented by your Customer Advisor (CA), who is your interface with the Rapid7 SOC and Threat Intelligence teams. Your CA will provide suggestions on managing your technical environment while offering tailored guidance and recommendations specific for your business to accelerate your security maturity.

Technology

The Rapid7 Managed Detection and Response service is powered by the Rapid7 Insight cloud, with endpoint data collected from the Insight Agent, a lightweight yet powerful software you can install on any asset—whether in the cloud or on-premises—to collect endpoint data from critical and remote assets across your IT environment.

The data passed to the analyst team by the Insight Agent allows the MDR analysts to get as close to the attacker as possible and perform endpoint investigations and threat hunts with system-level visibility. Combined with our Gartner-ranked cloud SIEM, InsightIDR, this endpoint data is parsed against real-time threat intelligence insights from the Rapid7 customer base and sophisticated behavioral analytics (tuned with an in-depth understanding of your business) to uncover threats across your internal network and cloud services.

Additionally, InsightIDR allows the MDR SOC team to integrate feeds from your existing security infrastructure, giving the Rapid7 MDR team even greater visibility into possible threats across your environment. As a customer of Rapid7 MDR, you'll have full access to InsightIDR, giving you visibility into the product and investigations and the ability to learn from the tool.

Process

Our expertise and technology reveals its true power when a threat is detected. Our MDR SOC analyst team uses a series of detection methodologies to validate each threat by gathering context related to the alert from your endpoints and logs to assess severity. Then we'll only report the true, real threats and suspicious lateral movement, and provide prioritized recommendations (e.g. containment, remediation, and mitigation actions) for your team in the form of a Findings Report. The result: MDR customers quickly identify and respond to attacker activity without wasting time investigating a mountain of false alerts.

What You Can Expect

Rapid7's approach ensures that there is full visibility and an organized response to incidents that occur in your environment. This encompasses four areas of service delivery with Rapid7 MDR:

Incident Detection & Validation

- 24/7/365 Monitoring
- Proactive Threat Hunting
- Initial Compromise Assessment
- Investigations of Threats and Alerts
- Alert Validation

Technology Access

- Full Access to InsightIDR Capabilities
  - SIEM
  - UBA
  - ABA
  - EDR
  - Deception Technologies
- Deployment Assistance Included
- No Additional Data Charges

White Glove Service

- Named Customer Advisor
- Threat Intelligence Team
- Custom Threat Profile
- As-it-happens Findings Reports
- Monthly Hunt Reports
- Monthly State of Service Reports
- As-it-happens Proactive Threat Reports

Incident Response & Escalations

- Process for Containment, Remediation and Mitigation of Threats
- Two Incident Escalations Included
- Slas for Threat Notification

Your Advantages With Rapid7 MDR

Rapid7's MDR offering goes far beyond the capabilities of traditional Managed Security Service Providers (MSSPs), who often provide incomplete technology solutions without the required expertise to manage the systems and provide guidance. Our belief in delivering the Rapid7 MDR service is to be more than a vendor, and for our team to do more than just alert you of threats. Counter to the Rapid7 MDR offering, the typical MSSP rarely offers threat hunting, and the experience is an impersonal one-size-fits-all approach that merely focuses on detection of malware and sending sterile tickets rather than a strict focus on advancing your security program. For more detailed analysis, please review our Rapid7 MDR vs. MSSP comparison brief.

Rapid7's Managed Detection and Response (MDR) service provides customers with five key advantages:

1. Improved Security Maturity

Rapid7 MDR is positioned to meet our customers at any level of security maturity and help accelerate that maturity, not just manage a SIEM. The team—from SOC analysts to your Customer Advisor—takes the time to truly understand your business processes, environment, and industry so they can provide customized guidance at each interaction point with the MDR service. This includes tailored reporting and recommendations, with remediation and mitigation strategies that align your investment in MDR with long-term security improvement across all 20 CIS critical controls. We go above simply looking at detection and response, with advice and mentorship from your Customer Advisor.

2. Powerful Agent and SIEM Technology

MDR is powered by the Rapid7 Insight cloud, with data fed from the Insight Agent to perform endpoint investigations and hunt for threats in your environment. This lightweight Agent unifies data collection for the MDR team to effectively view and correlate endpoint data, including: detailed asset information, Windows registry information, file version and package information, running processes, authentication information, local security and event logs, and more.

This is data is encrypted at rest and in transit as it's sent to InsightIDR for log correlation and investigation. Combined, the Insight Agent and InsightIDR provide the MDR team system-level visibility to spot real-time detections on the endpoint—the closest point to the attacker. As a customer of the MDR service, your team will have direct access to your instance of InsightIDR, giving you full transparency into our service and the ability to interact with the MDR team. Customers and their teams now have a single provider for both MDR services and SIEM/EDR technology.

3. Leading Threat Intelligence

Customer defenses leverage Rapid7's primary threat intelligence on attacker behaviors and common indicators of compromise, all powered by Rapid7's Managed Threat Intelligence Engine, cybersecurity research projects, vulnerability disclosures, insights from our customer endpoints, and Rapid7 SecOps Services engagements. In addition, Rapid7 leverages top third-party threat intelligence from security partners in the community, most notably Rapid7's involvement as an Affiliate member of the Cyber Threat Alliance (CTA) with Board and Committee seats.

4. World-Class Managed Services Team

The global MDR SOC teams are composed of security experts with unparalleled experience—both red team and blue team—with an assigned, primary high-tier analyst who becomes a subject matter expert in your user behavior, endpoints, and networks. Your analyst uses this in-depth knowledge of attacker tools, tactics, and procedures to catch malicious activity early in the attack lifecycle and validate each potential threat. Each of our SOC analysts acts as an extension of your security team and tailors the MDR service specifically to your industry and your business. This includes threat hunting, validation of threats, and guidance (e.g. containment, remediation, and mitigation recommendations) for only true threats.

5. Included Incident Escalation

Rapid7 offers two (2) Incident Escalations per year, giving MDR customers the ability to engage skilled personnel rapidly in the event of a compromise.

MDR Customer Engagement Model

The Rapid7 MDR team consists of multiple functional groups working together to ensure you receive world-class incident detection and response, providing 24/7 monitoring, unsurpassed service, and contextualized reporting that delivers real value.

We pride ourselves on becoming a true extension of customer teams through attentive service, visibility into our backend systems, and by providing a named resource (your Customer Advisor) whom you can reach out to for all things related to security.

Customer Advisor

Your **Customer Advisor (CA)** acts as a trusted advisor/ consultant. He or she should be considered an expert in your environment and a knowledgeable resource who can help your organization advance more securely. Customers Advisors will help your security team jointly manage the deployed cloud instance of InsightIDR while contextualizing alerts, investigations, and analysis.

Your CA is your main point of contact for the Rapid7 MDR service. This person has deep knowledge of your organization and works with you as a strategic security partner, from initial technology deployment through incident remediation. Having risen through the ranks of technical service delivery and customer success, each CA brings domain expertise, technical acumen, and white glove customer service. As such, customers often leverage their CAs as security experts to ensure their CISOs and board members are prepared to address any changes in the threat landscape.

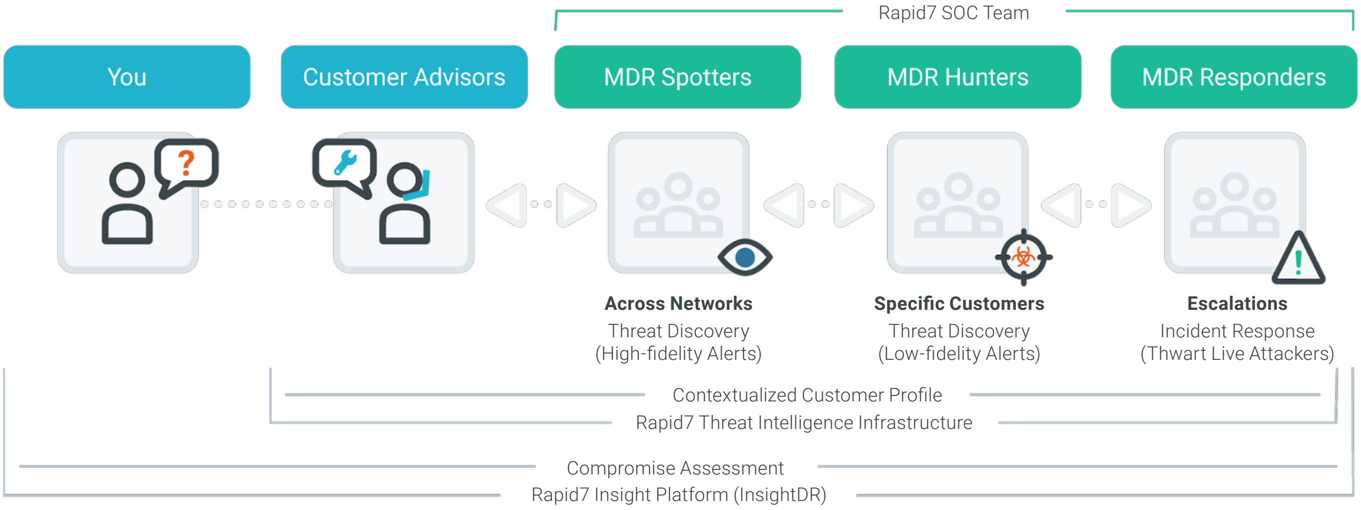
Throughout the service, your CA will communicate with you frequently via your preferred communication method and cadence, though never less than once a month. Typical communications provide updates on service delivery, walk you through Findings Reports, and assist you with reaching your security goals. Alternatively, you can proactively reach out to your named CA, or call the Customer Advisor hotline, whenever you'd like to chat about the service or your environment.

As part of the monthly check-in, Rapid7 will provide metrics and context surrounding analysis activities performed by the MDR analysts, technology health, and findings summaries. These reports serve as an at-a-glance overview of MDR activities. Additionally, the CA provides context for your MDR service and what any reports or threat intelligence insights mean for you and your business.

MDR SOC

Our SOC implements a three-tiered approach to ensure we have coverage for high- and low-fidelity alerts and can identify unknown threats through hunts in your environment. Together, the MDR SOC teams of world-class analysts maintain 24/7/365 vigilance of your network, from alert validation through in-depth forensics and malware analysis of your network and users. Our combination of these roles provides optimal coverage for all threats and attacker challenges.

- **Spotters** triage alerts across all customers to validate and report on high-fidelity indicators generated from InsightIDR (SIEM, EDR, UBA, ABA, deception technology), as well as the SOC's proprietary tools. Spotters typically monitor for simple threat intelligence matches and Attacker Behavior Analytics. Spotters typically have 2–4 years of experience validating and hunting for threats.
- **Hunters** are assigned to individual customer clusters to ensure a deep understanding of each of their customers' environments and threat profiles. Hunters are responsible for validating and reporting on lower-fidelity, technology-generated indicators like UBA and ABA alerts, as well as conducting monthly threat hunts. Hunters typically have 4–7 years of experience validating and hunting for threats.
- **Responders** support threat monitoring, hunting, and are responsible for leading incident escalations by providing advanced remediation and mitigation recommendations gleaned from deep analysis of evidence and malware. Additionally, these individuals assist in developing customer-specific detections (e.g. specific types of activities happening in the network) and work alongside our Threat Intelligence team to write new threat detections. Responders have 7+ years of cybersecurity experience, including incident response.



Threat Intelligence Team

Rapid7's **Threat Intelligence team** supports the SOC and CAs with analysis and new detections. Our MDR Threat Intelligence team are the vigilant researchers working on your behalf to identify new attacker trends before you are impacted. Our Threat Intelligence analysts provide customers and SOC analysts with the surrounding context needed to defend against threats with new detection mechanisms for vulnerability exploits and attack campaigns.

Additional Members of Rapid7's Team

A unique value point for Rapid7's MDR service is the strength and expertise of our employees who work with your organization to advance your security maturity. Throughout your service, you may come in contact with many of our excellent team members, including:

- **Account Executives:** Your introductory point of contact for all presale needs. The Account Executive takes the time to understand your business challenges, explains how our technology works to solve them, and proposes solutions to help accelerate your security maturity.
- **Project Managers:** The Deployment Project Manager leads MDR deployment coordination between Rapid7 and you, the customer. This person is responsible for ensuring a seamless experience during the deployment phase and can address any issues that arise during the deployment process.
- **Deployment Consultant:** Rapid7's InsightIDR solution specialist who is responsible for implementing and configuring the InsightIDR solution and for confirming configuration of all other related technology (e.g. log sources, event sources, collectors, etc.).
- **Customer Success Manager (CSM):** A Rapid7 CSM is assigned to your account for the entirety of your relationship with Rapid7. The CSM is an internal advocate who ensures your team's success by facilitating the best use of Rapid7 solutions and driving resolution on technology-related issues and requirements. This person is also your point of contact for adopting new Rapid7 solutions or expanding your solution coverage.
- **Security Operations Center (SOC) Manager:** Rapid7 SOC managers oversee and manage Rapid7 SOC operations, analyst teams, and MDR's internal infrastructure to ensure your ongoing success and coverage of your environment.

MDR Technology Overview

The Rapid7 MDR service leverages our InsightIDR solution to provide comprehensive protection against intruders in your internal network, devices, and cloud services. Additionally, the MDR SOC integrates event sources from your existing security infrastructure, granting the Rapid7 MDR team greater visibility into threats across your environment.

Customer-Deployed Software and Configuration

Insight Agent

The universal Insight Agent is lightweight software you can install on any asset—whether in the cloud or on-premises—to automatically collect data from endpoints (even those from remote locations that rarely join the corporate network) to enable the Rapid7 MDR team to have real-time visibility to identify malicious activity on your endpoints.

The endpoint agent enables our analysts and behavioral analytics tools to get as close as possible to the attacker, with the complete set of evidence needed to assess a threat. Each agent can be leveraged to perform on-demand containment actions to quarantine an endpoint asset or kill a process. We recommend deploying the Insight Agent on all endpoints, but require deployment on at least 80% of applicable assets using your existing software management processes in order to deliver service.

Rapid7 assigns deployment resources to work with you for the initial deployment of the Rapid7 MDR technology stack and ensure your event sources are configured for optimal coverage.

Insight Collector

The Insight Collector is responsible for receiving log data and agent data from your environment. All collected data is compressed and encrypted before being forwarded to the Insight cloud. The Collector also acts as a proxy for endpoint agents to reduce bandwidth constraints and increase endpoint scalability.

InsightIDR

Rapid7 MDR provides full access to jointly manage your InsightIDR instance, including access to functionality such as investigations, log search, dashboard cards, and reporting. Your team can also establish custom alerts in InsightIDR. Please note, however, that Rapid7 will be unable to act on these custom alerts beyond the monitoring that MDR typically covers. Your team should not modify or close out alerts within InsightIDR without first contacting your CA to ensure the Rapid7 MDR team maintains complete visibility.

InsightIDR also ingests data from multiple event sources, each configured in InsightIDR to create a unique log in Log Search. The standard MDR subscription includes 13 months of hot, immediately searchable log data and storage. Longer term retention is fully available to meet your business and compliance needs. Since the Insight architecture runs in the cloud, no external hardware is required for storage.

Event Sources

You are required to connect logs for four foundational event sources to the Insight Collector(s): Active Directory (for Windows assets), DHCP, DNS, and LDAP directory services (or equivalent as agreed upon with Rapid7). Rapid7 will validate connectivity and processing once deployment is complete. Rapid7 will also perform ongoing monitoring to evaluate the health of the technology stack and provide you with notifications when a failure or issue is identified.

Deception Technology (optional)

InsightIDR comes included with honeypots, honey users, honey credentials, and honey files designed to identify malicious behaviors using fake assets, users, credentials in memory, or files.

Rapid7 Cloud Technology Architecture and Capabilities

Insight Cloud

Responsible for all log management, data processing, enrichment, and storage of customer data aggregated from each endpoint with the Insight Agent. Each customer instance on the Insight cloud is isolated from other instances.

InsightIDR

Rapid7's purpose-built cloud SIEM for incident detection and response combines real-time threat intelligence insights with a deep understanding of your environment and sophisticated behavior analytics to identify threats. InsightIDR aggregates endpoint behavior, user behavior, and log history in a single solution offering a comprehensive view of the core technical environment.

Rapid7 Threat Intelligence Infrastructure

Primary Rapid7-developed intelligence paired with additional third-party sources to enrich the attack detection and response processes in near real time. This intelligence is fed back into the InsightIDR solution to update the behavioral analytics and detections within the product. A full review of Rapid7's Threat Intelligence infrastructure can be found here.

Services Workflow and Process

Rapid7's Managed Detection and Response service engagement is provided in four phases:

1. Detection

Rapid7 MDR leverages pre-built detections in InsightIDR combined with our threat intelligence engine and proactive threat hunting to identify both known and unknown threats before they can cause material impact. See all detection methodologies.

Rapid7 InsightIDR, in turn, leverages thousands of pre-built detections to identify intruder activity, cutting down false positives and enabling analysts to only alert you to true threats.

Additionally, InsightIDR baselines all users and actions to augment pre-defined rules to better detect anomalous and concerning activity. These behavior analytics detections are bolstered with:

Intruder traps

Honeypots, honey users, and honey credentials—built alongside our industry-leading offensive security/hacking team (pen testers) and knowledge from the Metasploit Community—to understand how best to plant traps attackers couldn't resist interacting with.

Explicit attack behavior indicators

InsightIDR uses advanced analytics to detect compromised users/assets that don't require an established baseline of behavior to trigger. One example is the ability to detect spear phishing attempts where the domain has been spoofed (i.e. rapid7.co instead of rapid7.com).

Additional data sources

InsightIDR integrates with your third-party offerings to identify suspicious processes, URLs, hosts, and IPs.

2. Investigation and Validation

Rapid7 validates alerts based on two key factors: attacker intent and observed capability. By combining adversary threat intelligence and knowledge of attack tools, Rapid7 determines the risk and potential impact of each incident and delivers that context in detail.

Each critical alert triggered by InsightIDR is manually triaged by our expert SOC analyst team to ensure validity. Our multi-layered process weeds out benign events, allowing our MDR team to **only report threats that are actually considered malicious** and need direct actions to be taken. This enables our team to produce near 0% false-positive reports and offer actionable guidance with tailored recommendations for your team to take on confirmed threats, including direct containment from within the reports and InsightIDR.

3. Reporting

Once alerts are investigated and verified, our SOC analysts produce a **Findings Report** delivered via the Customer Services Portal (with alerts via email or phone call, per the customer's request). This report is a summary of the incident with detailed evidence of the threat, recommended containment actions, remediation guidance, and mitigation recommendations.

The following additional reports are provided on a one-time, monthly, or an ad-hoc basis based on actions in your environment:

Compromise Assessment (one-time basis upon deployment)

The Compromise Assessment report contains any detected active or historic compromises, potential avenues for future breaches, and remediation and mitigation recommendations.

Service Reports (monthly)

Rapid7 will provide you with metrics and context for analysis activities performed by the MDR analysts, as well as technology health and findings summaries. These reports serve as an at-a-glance overview of MDR activities.

Hunt Reports (monthly)

Hunt Reports contain metrics and findings related to proactive threat hunts using analyzed data from our endpoint metadata and forensics collected by the Insight Agent to identify persistent malware, historical application execution, unusual processes and network communications, and per-system anomalies.

Threat Intel Report (ad hoc)

A highly targeted analysis that leverages the power of our threat intelligence infrastructure, including Project Heisenberg, Project Sonar, and third-party threat intel with a global footprint to monitor and detect patterns in the wild. Many of these findings could impact your environment; we'll use this information to develop rules to scan your environment, which can be used to perform more real-time asset hardening.

Threat Intel Research Report (ad hoc)

This report is generated by the Threat Intelligence team and can include information on the threat landscape, activity observed in the wild, industry trends, and behavior of specific actors. Often these reports are requested for key briefings, to help prepare teams for potential attacks, and to focus resources on critical risks.

Incident Escalations Reports (in the event of an escalation)

In the event we need to escalate a breach into Incident Escalation, our team keeps you informed of our progress through various reports detailed in phase 4 below.

4. Escalation (On-Demand)

In the event of a validated breach during or after the Compromise Assessment and during the monitoring phase of your contract duration, Rapid7 will contact you with the option to exercise one of your **two (2) Incident Escalations each year** included in your MDR service per your contract, per the service level objectives outlined below:

ESCALATION ACTIVITY	TIME TO ACTION
Time to Begin Escalation	1 hour from initiation of incident escalation
Communications and Updates	Daily updates, along with a daily debrief of the day's investigation results and progress. Substantial findings will be communicated regularly as they are discovered
Incident Escalation Report	Within 2 business days from completion of investigation

An Incident Escalation is a technical process handled by the Managed Services SOC. An Incident Escalation is triggered when a customer is compromised. All investigation activity is conducted remotely and limited to examination of data obtainable by the InsightIDR Insight Agent and platform. Disk forensics are not included as part of an Incident Escalation.

Rapid7 MDR allocates SOC analysts for each Incident Escalation event. Activities performed during an Incident Escalation include:

- **Remote technical analysis and incident scoping:** The MDR team leverages Rapid7 cloud services and the Insight Agent to perform a remote incident investigation and scope attacker activity.
- **Daily reporting:** Rapid7 will provide a daily status report during the duration of the Incident Escalation detailing new findings and recommendations.
- **Final report:** At the conclusion of the Incident Escalation, Rapid7 will provide a final report detailing attacker activity supported by evidence with remediation and mitigation recommendations.

Unlike Incident Response services offered through the Rapid7 Global Services team, the investigation and output for Incident Escalations is done remotely and is limited to examination of data obtained by the Insight Agent and InsightIDR. If your incident falls outside the scope of an Incident Escalation (e.g., pre-dating the start of your MDR service, on-site help is needed, data collected outside of InsightIDR or the Insight Agent), or you wish to escalate more than two (2) incidents per year, Rapid7 will offer Incident Response services at a daily or weekly rate, as applicable per a separate Incident Response Services contract. You can work with your Account Executive to purchase an Incident Response retainer or to engage Rapid7's Incident Response services at the time of the incident for an hourly time and materials rate.

Escalation Protocol

Should a threat require an incident escalation detected by the Rapid7 MDR team, your Customer Advisor will request authorization to execute the incident escalation and additional analysis and reporting will begin. Additionally, in the event your team identifies an internal security incident and requires Rapid7 Incident Escalation assistance, you can contact your CA to begin the Escalation process.

Once you have transitioned to Incident Escalation, the Managed Detection and Response team and Rapid7 Incident Escalation teams will analyze the security incident to identify the scope of compromise, affected systems and accounts, malware used by the attacker, and attacker command and control channels.

A complete workflow outline is available here.

MDR Service Deliverables

Compromise Assessment

Following completion of the Deployment phase, Rapid7 will conduct a Compromise Assessment prior to your MDR service initiation to ensure there is not active malicious activity in your environment or evidence of previous compromise(s). Additionally, the Compromise Assessment allows our SOC analysts to familiarize the Rapid7 team with your security environment and provide actionable recommendations to bolster your security posture, and—if enacted—reduce the risk of future compromise.

The Compromise Assessment appraises your environment to validate evidence of attacker infiltration, active or historic compromises, potential avenues for future breaches, and actionable steps for remediation and mitigation, including:

- **Operating system-specific malware persistence mechanisms and process injection methods:** We review currently running processes, scheduled tasks, and common hiding places to detect anomalies in behavior and communications.
- **Attacker lateral movement:** We apply threat intelligence and User Behavior Analytics to uncover the attacker pathway in real time by analyzing common attacker behaviors, including compromised credentials and ingress from suspicious locations.
- **Common attacker tools:** We find evidence of attacker activity, including modified registry keys or executable files left behind, to validate suspected compromise.
- **Indicators derived from investigations:** We evaluate an exhaustive list of compromise indicators, such as privileged user account anomalies, or suspicious registry changes. InsightIDR detections are constantly updated with IoCs from MDR investigations, Incident Escalations, pen testers, Incident Response team engagements, and Rapid7-hosted events (e.g. Capture the Flag challenges) to improve the product's capabilities to detect anomalous activities.
- **Environment-specific considerations:** We take the time to understand your environment and the relationships between users, hosts, and processes (UHP) to identify any artifacts in the kill chain.

A sample Compromise Assessment Report can be viewed here.

Findings Reports

For each validated incident in your environment, within one (1) hour of validating that incident, Rapid7 will produce a Findings Report containing:

- Investigation details
- Written analysis
- Incident criticality
- Containment recommendations (how to contain the endpoint or user)
- Remediation recommendations (how to resolve this finding)
- Mitigation recommendations (potential ways to prevent future recurrence)

A sample Findings Report can be viewed here.

Monthly Service Reports

On a monthly basis, Rapid7 will provide you with metrics and context for analysis activities performed by the MDR analysts, as well as technology health and findings summaries. These reports serve as an at-a-glance overview of MDR activities. The Customer Advisor will review this monthly recap summary with all stakeholders of MDR on the scheduled monthly call to make recommendations to reduce risk over time.

A sample Monthly Service Report can be viewed here.

Threat Hunt Reports

Each month, Hunter SOC analysts leverage the Rapid7 Insight Agent to collect metadata from multiple locations on your endpoints to proactively identify persistent malware, historical application execution, unusual processes and network communications, and per-system anomalies. The findings of these proactive threat hunts will uncover unknown threats in your environment and present data from the MDR analyst's forensic acquisition including, but not limited to:

- Evidence of threats from MDR-curated indicators of compromise
- Remote access solutions
- Cloud storage solutions
- Potentially unwanted programs (PUPs)
- Administrator utilities
- PowerShell invocation
- Webshell activity
- Lateral movement
- Ingress authentication
- Server Message Block (SMB) egress
- Potentially vulnerable open ports

A sample Hunt Report can be viewed here.

Threat Intelligence Reports

When Rapid7's Threat Intelligence infrastructure or third-party threat intelligence partners identify new vulnerabilities or detection patterns, the Rapid7 team will publish a detailed analysis of the threat to inform you of the findings. The purpose of this report is to help you better understand the global risk environment. The MDR team leverages this information to develop rules to scan your environment.

A sample Threat Intel Research report can be viewed here.

Incident Escalation Reporting

In addition to the reports provided by Rapid7 for each threat identified in your environment, Rapid7 MDR offers resources to help with up to two (2) incident escalations per year when it's recommended to remove attackers from the environment.

For Incident Escalations, Rapid7 will work with your team to identify a scope specifically tailored to the identified threats, and continue to remotely investigate and provide detailed reports during and at the conclusion of the escalation, including:

- **Remote technical analysis and incident scoping:** Rapid7 will leverage the Insight cloud and the Rapid7 Insight Agent to perform a remote investigation of the incident and scope attacker activity related to the incident.
- **Daily reporting:** Rapid7 will provide a daily status report during the duration of the incident escalation detailing new findings and recommendations.
- **Final report:** At the conclusion of the Incident Escalation investigation, Rapid7 will provide a complete report detailing all attacker activity, supported by evidence and recommendations to remove the threat from your environment.

Service Level Objectives (SLOs)

Alert Priority

The Rapid7 Threat Intelligence team and the MDR SOC work closely together to tune detections and ensure they are as high-fidelity as possible. In addition to tuning alerts to minimize alert noise, Rapid7 also assigns an internal priority for all alerts. This internal priority ensures that the alerts generated by high-fidelity detections and likely to result in a Critical or High criticality are highlighted for expedited SOC triage and investigation.

The Rapid7 MDR SOC triages Critical and High priority alerts in the order of severity to ensure the most pressing threats are identified and that remediation, mitigation, and containment guidance is offered. This allows the team to reduce the likelihood an attacker will gain a foothold and perform malicious activities, while also reducing the burden on our SOC team to investigate benign and false-positive alerts over actual suspicious or malicious events.

Alert Validations

The Rapid7 MDR SOC determines event criticality during the course of an investigation into an identified event. It is not possible to assign criticality before the scope of the event is determined.

Validation is defined as the Rapid7 MDR SOC performing initial triage and investigation to determine, with a high degree of confidence, that the event is non-benign and requires customer communication.

SEVERITY LEVEL	EXAMPLE BEHAVIORS	TIME TO NOTIFICATION	TIME TO FINDINGS REPORT
Critical	An incident created via non-commodity malware deployed via spear phishing, social engineering, zero-day exploitation, or strategic web compromise, specifically targeted towards a target or organization.	Within one (1) hour of validation; Ongoing communications as they become available, but at a minimum, every 4 business hours. Significant findings will be communicated as they are identified.	Within 24 hours upon completion of investigation.
High	An incident created using targeted off-the-shelf software backdoor deployed via spear phishing, social engineering, or strategic web compromise. Planned and targeted, but using common malware.	Within one (1) hour of validation; Ongoing communications as they become available, but at a minimum, every 4 business hours. Significant findings will be communicated as they are identified.	Within 24 hours upon completion of investigation.
Medium	An incident created using common threat malware, typically non-specifically targeted, but rather opportunistic and automatic.	Within eight (8) hours of validation; Ongoing communications as they become available, but at a minimum, every 8 business hours. Significant findings will be communicated as they are identified.	Within 24 hours upon completion of investigation.
Low	An low-risk threat, not capable of remote code execution, credential harvesting, or data theft (e.g. spam email delivering adware).	Within eight (8) hours of validation; Ongoing communications as they become available, but at a minimum, every 8 business hours. Significant findings will occur as they are identified.	Within 24 hours upon completion of investigation.

Insight Cloud Uptime

Rapid7 MDR leverages the Insight cloud, Rapid7's industry-leading security platform, to deliver the MDR service. As such, the uptime availability of this technology reflects that of Rapid7's overall Insight cloud Service Level Agreement.

Customer Advisor Response Times

Your Customer Advisor is held to the following SLOs for notifications and responses to inquiries from your team:

- One (1) hour to proactively reach out to you for validated critical or high severity threats by phone to provide the relevant details quickly while the SOC team generates a Threat Report.
- Two (2) business hours to respond to an urgent request from your team at the discretion of your Customer Advisor.
- One (1) business day to respond to a non-urgent request from your team at the discretion of your Customer Advisor.

Incident Escalation Procedure

In the event of an Incident Escalations, the Rapid7 MDR team will begin the Incident Escalation within one (1) hour once you have approved the escalation.

90 Day Success Plan

We work with our customers to deploy as quickly as possible to shorten the time to value, and as such we rely on our customers to ensure all necessary tasks are completed on their end. All required actions are outlined in the deployment timeline below; customers with smaller asset counts can often experience a shorter timeline in launching the MDR Service.

30/60/90 Day Success Plan

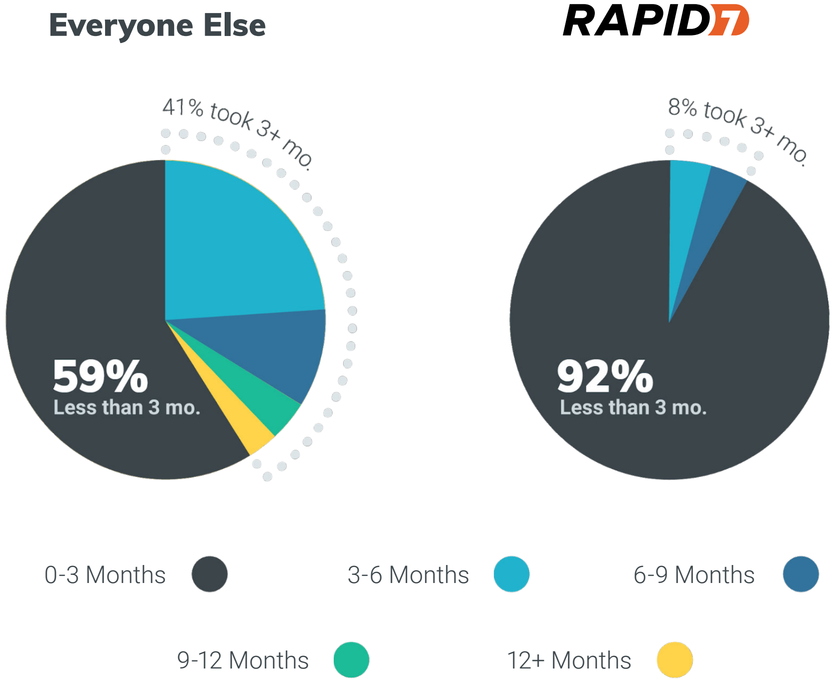
Customers should expect the following for 30/60/90 day milestones and operational results as a Rapid7 MDR customer:

MILESTONES	OPERATIONAL RESULTS
30 DAYS	
• Welcome email • Access to InsightIDR • Deployment kickoff call • Agent deployment completed • Collectors and foundational event sources configured	• Deployment completed • Product training and education completed
60 DAYS	
• Learn environment/start building threat profile • Start monthly meetings and reviews	• Product baselining • Compromise Assessment completed • Threat hunting now active • Log search available across all sources • All pre-build alerting is active
90 DAYS	
• Continue operational cadence and continued monitoring	• Monthly alert roll-up • Proactive threat hunt findings • Threat intelligence review • Quarterly goal review • Open Q&A and engagement with Rapid7 experts

MDR Technology Deployment

InsightIDR SaaS Advantage

As the only true SaaS SIEM on the market today, InsightIDR deploys faster then competing SIEM solutions. With this advantage, our team is able to stand up our MDR service within weeks.



Source: Gartner Peer Insights

Customers that already have the Insight Agent deployed in their environment significantly reduce the level of effort required to be 100% optimized as a Managed Services customer.

MDR Launch Phases

Rapid7 MDR Onboarding in broken into three distinct phases, including:
One (1) week of initiation activities (“Initiation”)
Four (4) weeks of deployment activities (“Deployment”)
Four (4) weeks of hunt/baselining activities (“Baselining”)

Once Deployment, Baselining, and the Compromise Assessment are completed, Rapid7 will commence the monitoring and threat assessment phase (“Monitoring”) as an ongoing service delivery.

Initiation Phase

The Initiation phase will introduce you to the setup and launch team, which includes a Project Manager, Operations Coordinator, and Security Consultant. The team works with your Rapid7 onboarding Project Manager to start the onboarding process.

TASK	MDR MILESTONES	DURATION	DETAILS
1.1	Welcome Email to Customer from Managed Services	1 day	Onboarding Team will send
1.2	Set up Customer in InsightIDR Portal	1 day	Customer will receive Log In details for InsightIDR via email
1.3	Set up Customer in Customer Portal	1 day	Customer will now have access to Customer Portal to access Site Survey
1.4	Enable Support Credentials	1 day	Enable support credentials for Customer
1.5	Welcome Email to Customer from Operations Manager	1 day	Introduces Project Manager and sends link for Kick Off Meeting Calendar options
1.6	MDR Kick Off Call	1 day	Define specific roles and responsibilities of the customer during the deployment and ongoing engagement phase
1.7	Complete Site Survey	1 day	If not already completed in PreSales, the Project Manager will ask you to complete a site survey

Initiation→ Deployment

To move from Initiation to Deployment, the following checkpoints must be completed:

- Configuration of InsightIDR and the Customer Portal
- Introductory Managed Services Kickoff Call
- Site Survey Response Submitted to the Customer Portal

Your MDR service kickoff call will include:

- Managed Services and Technology Delivery Overview
- Customer Engagement Model
- Defining Your Incident Escalation Process with Rapid7

Deployment Phase

Deployment phase is split into two stages:

- InsightIDR Setup with Collectors and Agents Deployed
- Validation of InsightIDR Setup

During your deployment, Rapid7 will provide one to two days of remotely dedicated time with our deployment consultant to assist in configuring your event and log sources into the platform service. During this stage, the Rapid7 deployment team will also help your team set up dashboards inside the InsightIDR product.

Following this, the Rapid7 team will provide best practices training and help configure advanced configurations in the InsightIDR dashboards. It is important to ensure you're following the recommended deployment requirements for successful deployment.

InsightIDR Setup Collectors, Agent, Event Sources

TASK	MDR MILESTONES	DURATION	DETAILS
2.1	Set Up Collector(S)	1 day	Use the wizard in InsightIDR to set up first Collector
2.2	Deploy Rapid7 Insight Agent to All Servers and Workstations	2 weeks	Deploy Agents using Token Installation
2.3	Configure all Foundational Event Sources	2 weeks	DHCP, LDAP, DNS & AD required for MDR Service
2.4	Deployment Event Sources	2 days	Customer will be invited for 1 or 2 full days with the Deployment Consultant to configure and validate all Event Sources and prerequisites. It is also an opportunity for training and education on InsightIDR

Validate InsightIDR Setup

TASK	MDR MILESTONES	DURATION	DETAILS
3.1	Verify Collectors & Agents	2 days	Deployment must be to at least 80% of asset environment
3.2	Configure/Validate Event Sources	2 days	
3.3	Custom Event Source Syslogs	2 days	
3.4	Set Up Deployment Phase Artifacts	2 days	
3.5	Set Up Custom Alerts, Dashboards	2 days	
3.6	Log Search Overview	1 day	

Deployment→ Baselining

There are two major prerequisites to move from Deployment to Baselining during onboarding:

1. Four foundational event sources configured

- Domain name system (“DNS”)
- Active directory (“AD”)
- Dynamic host configuration protocol (“DHCP”)
- Lightweight directory access protocol (“LDAP”) (collectively, the “event sources”)

2. Minimum of 80% of your environment covered by the Rapid7 Insight Agent

Baselining Phase

Your Rapid7 Customer Advisor (CA) will take over for the Rapid7 Deployment team and introduce the next phase of onboarding: Baselining. The Customer Advisor will be your primary contact onwards in connection with the MDR service and the platform service.

TASK	MDR MILESTONES	DURATION	DETAILS
4.1	Monitoring Kickoff Call	1 hour	CA invites the Customer to a Monitoring Kick Off call to introduce the next phase of the Service. The CA will explain the reports that Customer will receive on an ongoing basis and set-up communications protocols and processes as defined by the Customer.
4.2	Set up Customer in Security Operations Center ("SOC") Tool		
4.3	SOC Notified Customer Ready for Baselining	1 day	
4.4	SOC Analyst Assigned	1 day	
4.5	Baselining Period	2 weeks	
4.6	Findings Report Created (if applicable)	1 hour	During Baselining, if malicious threats are found (such as an active malware event or if SOC notices the presence of an adversary) a Findings Report will be created for each threat as soon as they are discovered.
4.7	Hunt Period	2 weeks	
4.8	Deliver Compromise Assessment	1 day	This report contains any detected active or historic compromises, potential avenues for future breaches, and prioritized remediation and mitigation recommendations.

Baselining→ Monitoring

After the first two (2) weeks of MDR monitoring, InsightIDR will be configured to understand typical user, asset, and account behaviors. At the completion of Baselining, InsightIDR will understand the interactions between IP addresses, machines, and the user accounts on those machines. This baseline also starts to identify regular users from service accounts and admin accounts.

Additionally, at the end of the Baselining phase, Rapid7 MDR delivers a Compromise Assessment report that identifies and validates potential or present threats to your system environments, and will be continuously monitored using the platform service and other tools.

Monitoring Phase/Ongoing Service Delivery

Once Baselining is complete, your environment will be monitored by the Rapid7 MDR SOC, commencing the ongoing Monitoring phase. At this point, Rapid7 will deliver Findings Reports within 1 hour of a validated threat being confirmed.

TASK	MDR MILESTONES	DURATION	DETAILS
5.1	Service Reports	Monthly	Rapid7 will provide you with metrics and context surrounding analysis activities, technology health, and findings summaries for an at-a-glance overview of MDR activities.
5.2	Hunt Reports	Monthly	Our analysts leverage the Rapid7 Insight Agent to collect metadata from multiple locations on your endpoints to identify persistent malware, historical application execution, unusual processes and network communications, and per-system anomalies.
5.3	Threat Intel Reports	Ad-hoc	Highly targeted analysis that leverages the power of Rapid7's threat intel infrastructure (Project Heisenberg, Project Sonar, 3rd-party threat intel) to develop rules to scan your environment and perform real-time asset hardening.
5.4	Finding Reports	Ad-hoc	Findings reports provide written analysis, criticality, raw details, remediation recommendations, suggested containment actions, and mitigation recommendations for each validated incident.

APPENDIX

Detection Methodologies

Rapid7 MDR SOC employs a multi-layered approach to detect malicious activity across the attack chain for both known and unknown threats. Each detection through InsightIDR is validated by our SOC analysts to ensure we only pass true threats in our reports. This section will outline our detection methodologies, the role of InsightIDR in our threat detection, and the deliverables you can expect from the MDR team.

In order to have complete coverage, the InsightIDR technology integrates with your existing network and security stack to collect and query endpoints through the Insight Agent and endpoint scan. Beyond the alerts identified by InsightIDR, the MDR team also runs regular threat hunts in your environment and curates custom Threat Intelligence.

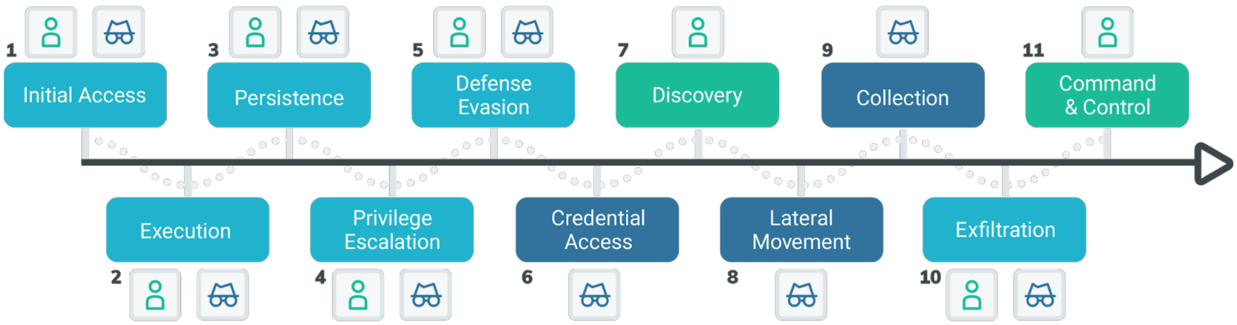
Behavior-based Detections

For our SOC team, detecting threats using InsightIDR is a core differentiator for Rapid7's MDR service, and it lays the foundation for advancing your security program's maturity by overlaying behavior-based detection methodologies.

The detection our team provides across the attack chain stems from a combination of User and Attacker Behavior Analytics, endpoint data, and deception technology.

Rapid7 MDR Aligns to MITRE ATT&CK Framework

User Behavior Analytics (UBA): Attacker Behavior Analytics (ABA):



Effective implementation of user- and deviation-based detection methodologies requires deep visibility into endpoints, network metadata, authentication/authorization events, and logs, coupled with purpose-built technology and subject matter expertise provided by the Rapid7 SOC.

User Behavior Analytics (UBA)

User Behavior Analytics (UBA) enables our SOC team to more easily determine whether a potential threat is an outside attacker impersonating an employee or an actual employee who presents some kind of risk, whether through negligence or malice.

UBA connects activity on the network to a specific user as opposed to an IP address or asset. This is then compared against a normal baseline of event activity for that user. Once collected and analyzed, it can be used to detect the use of compromised credentials, lateral movement, and other malicious behavior.

Our SOC leverages these UBA indicators to dynamically prioritize and rank alert criticality based on the presence or absence of notable behaviors associated with the alert by:

- **Detecting unknown threats** based on single occurrences, or groups of notable events based on specific user behaviors or deviations from known-good baselines.
- **Detecting insider threats** based on groups of notable events describing the sequence of events typically associated with information theft by an authorized party.
- **Associating user behaviors** based notable events to alerts and investigations to improve the validation and investigation analyst workflows.
- **Providing the data needed to associate technical evidence** with human understandable behavior for threat reporting.

InsightIDR provides our SOC team with a technological advantage by utilizing our proprietary attribution engine with models that are purpose-built to detect behaviors indicative of true threats, while sorting out users who may be doing unusual tasks but are not actually compromised or performing malicious actions. Many traditional SIEM solutions claim to utilize UBA detections, but SIEM engines aren’t built for real-time attribution, unlike Rapid7’s InsightIDR technology. This is because users and assets constantly move around in a modern network architecture, leading to an engine that cannot accurately map events to entities.

Attacker Behavior Analytics (ABA)

Attacker Behavior Analytics (ABA) applies Rapid7’s existing experience, research, and practical understanding of attacker behaviors to generate investigative leads based on known attacker tools, tactics, and procedures (TTP). These include:

- Malware, malware droppers, maldocs, and fileless malware (opportunistic and targeted)
- Cryptojacking (stealing CPU cycles to mine cryptocurrency)
- Pen testing and attack tools
- Suspicious persistence
- Anomalous data exfiltration
- New attacker behavior

ABA detection methods are constantly updated by MDR SOC investigations, combined with Rapid7’s research and threat intelligence analysts to extract key behaviors from threats identified in our customer environments. After performing research on related attacks and behaviors, we craft new ABA detections that are deployed across all MDR customers to simplify and accelerate detection and reduce the time to remediation. These sources include:

- MDR customers
- The Metasploit Community
- Project Heisenberg (our honeypot network)
- Project Sonar (our internet-side scanning project)
- Incident Response engagements
- InsightIDR customers sharing intel
- Rapid7’s Threat Intelligence team and community (e.g. Cyber Threat Alliance)

Other key advantages include:

- **Found once, applied everywhere:** Your security team gets the benefit of the learnings from other MDR customer investigations. When our SOC team finds new attack methodologies—either by way of our SOC, threat intelligence team, or Rapid7 research—those TTPs are updated in InsightIDR and applied to all MDR customers and investigations
- **Detections based on behaviors, not signatures:** Through InsightIDR, our SOC team is armed with high-fidelity endpoint data to identify novel variations of new attacker techniques.
- **High-fidelity alerts grant context to take action:** Alerts include context from our analysts and threat intel teams, so you can make better decisions, remediate the problem, mitigate risk, and contain the alert from directly inside your Findings Report.
- **Constantly evolving ABA detections:** Whenever possible, the alert will detail known, recent adversary groups using a similar technique in a confirmed attack.

As a key advantage of our cloud deployment model, our detections are updated automatically to our entire user population—including MDR customers—after a thorough prototyping, testing, and validation process. All new indicators are applied to one month's historic data so your environment is instantly protected.

Threat Intelligence-based Detections

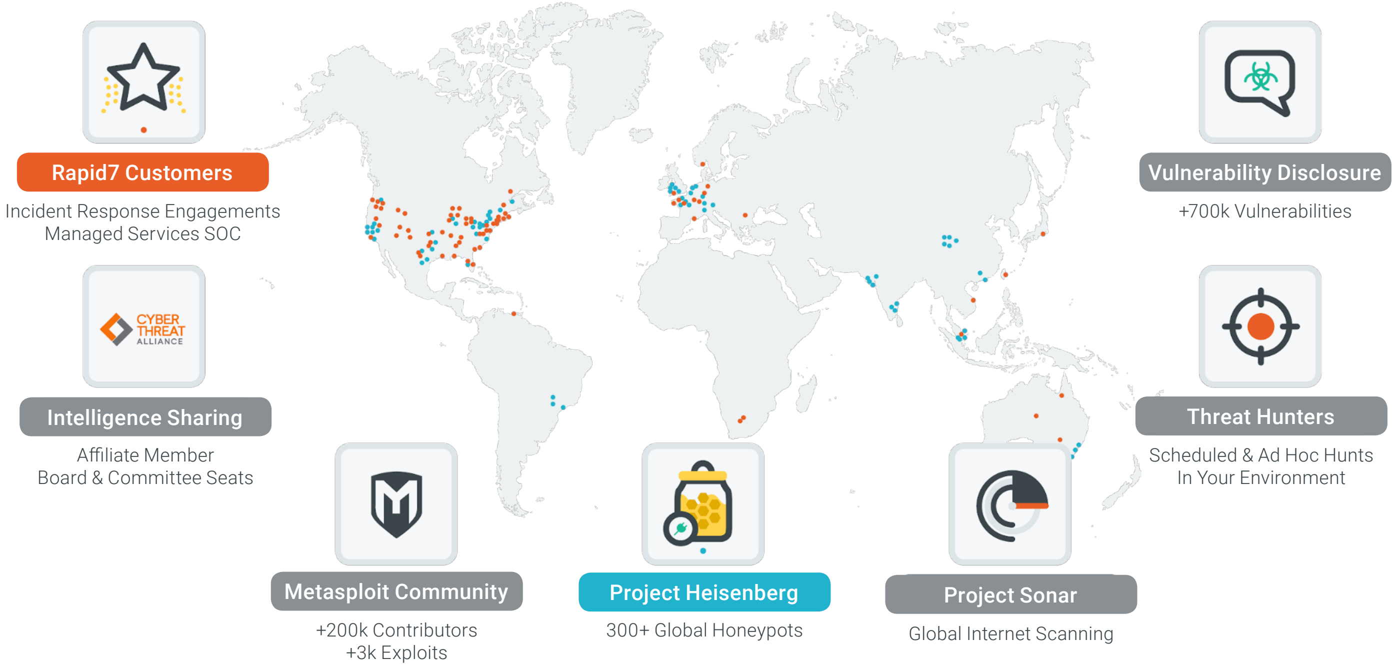
Rapid7 leverages proprietary threat intelligence derived from research, previous investigations and monitoring findings, as well as third-party sources. The MDR Threat Intelligence team is responsible for maintaining this intelligence and working alongside our SOC analysts to constantly apply threat detection and incident response learnings across all MDR customer environments.

Rapid7's Threat Intelligence team brings expertise and data sources from the public sector, private sector, and open sources to fuel threat detection and incident response.

- **Strategic threat intelligence** is provided per industry sector and is aimed at decision-makers to help shape strategies to prevent threats from materializing.
- **Tactical threat intelligence** is applied in our attacker behavior analysis methodologies and leverages complex rules to generate investigative leads across multiple event sources and over time.
- **Operational threat intelligence** is provided by way of proactive threat reports and indicates the likelihood of an impending attack. Our reports include mitigation recommendations to increase resilience against specific threats to your organization.
- **Technical threat intelligence** in the form of indicators of compromise are applied across our customer base. The Rapid7 Threat Intelligence team actively maintains the quality of the technical threat intelligence to ensure fidelity, context, and timeliness for our MDR threat analysts.

Rapid7 Research and Threat Intelligence Sources

We're committed to openly sharing security information that not only helps the entire cybersecurity community to learn, grow, and address issues in the security world, but also to improve our products and detections. Below are the common sources that lead to Rapid7's security expertise and intelligence advantage:



Rapid7 Customers
Incident Response Engagements
Managed Services SOC

Intelligence Sharing
Affiliate Member
Board & Committee Seats

Metasploit Community
+200k Contributors
+3k Exploits

Project Heisenberg
300+ Global Honeypots

Project Sonar
Global Internet Scanning

Threat Hunters
Scheduled & Ad Hoc Hunts
In Your Environment

Vulnerability Disclosure
+700k Vulnerabilities

- **Rapid7 customers:** Our detections are enhanced from learnings across our 1MM+ customer endpoints, MDR customers, and Incident Response engagements.
- **Intelligence sharing:** Rapid7 is part of the Cyber Threat Alliance (CTA), a community of security research organizations with a mission to improve cybersecurity cooperation to improve defenses against cyber adversaries. Rapid7 is an Affiliate member of the CTA with Board and Committee seats.
- **Metasploit Community:** Metasploit is the world's most-used penetration testing software used to uncover weaknesses in defenses with over 3,000 exploits and over 200,000 active contributors.
- Project Heisenberg **Cloud:** A collection of over 200 low-interaction, global honeypots distributed both geographically and across IP space. The honeypots offer the front end of various services to learn what other scanners are up to (usually no good), and to conduct "passive scanning" to help enhance our understanding of attacker methods.
- Project Sonar: A security research project by Rapid7 that conducts internet-wide scans across different services and protocols to gain insight into global exposure to common vulnerabilities.
- **Pen test engagements:** Rapid7 service engagements allow us to leverage real-world experiences of our engineers and investigators gathered over thousands of pen tests.
- **Vulnerability disclosure:** Rapid7 publishes our data for free to encourage scientists, engineers, and anyone else interested in the nature and form of the internet to make their own discoveries.

Human Validation

All events are validated by our SOC analyst team prior to reporting any alert to you. With human validation from our Spotters or Hunters, our MDR service removes benign, unnecessary, or redundant alerts from your Findings Reports.

Threat Hunting

Rapid7's MDR team leverages Insight Agent data and specialized views to perform scheduled and ad-hoc threat hunts in your environment. The nature of the hunts varies over time and is based on trends in the threat landscape. The results of these hunts are sent to your team in the form of the monthly Hunt Reports.

Requirements for Successful Deployment

To get the most out of your MDR deployment, Rapid7 encourages you and your team to adhere to the following responsibilities:

- Designate and assign a project manager or similar to work with Rapid7 for your deployment.
- Designate and assign a primary point of contact and escalation path for reporting incidents.
- Complete a Deployment Survey prior to starting the Deployment phase.
- Ensure availability of deployed technology on site, including: Insight Collector, log sources, optional deception technology, and Insight Agent; as well as their ability to report to Rapid7 infrastructure.

Additionally, Rapid7 will take on the following requirements to ensure a smooth deployment process:

- Provision the Rapid7 cloud services in the technology stack for your environment.
- Designate and assign a Customer Advisor to support your security maturity and be your trusted point of contact for all things MDR.
- Designate and assign a Customer Success Manager.
- Designate and assign a Rapid7 Project Manager.
- Provide adequately trained/certified staff to conduct the service including:
    - Working with your appointed project manager to schedule meetings and tasks.
    - Assist you with subject matter expertise to deploy the various required and optional technology stack components.
    - Monitor your environment 24x7x365 in accordance with Rapid7's MDR detection methodologies and within the scope of the visibility provided by the technology stack.

During Initiation, Deployment, and Baselining Phases, Rapid7 will complete the following deliverables:

- Supported event sources
- As-built guides
- Findings Report
- Monthly State of Service
- Monthly Hunt Report
- Site survey

About Rapid7

Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. 7,800 customers rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations. For more information, visit our website, check out our blog, or follow us on Twitter.