



CITY OF EVERETT
PROCUREMENT DIVISION
2930 Wetmore Ave., Ste. 9-E
Everett, WA 98201
425.257.8840

INVOICE
TO

ACCOUNTING DIVISION
P.O. Box 12130
Everett, WA 98206-2130
425.257.8746
accountspayable@everettwa.gov

ORDER SUBJECT TO TERMS LISTED ON LAST PAGE

PURCHASE ORDER

P.O. No. CB 24231

SUPPLIER NAME AND ADDRESS

40916
CRITICAL INSIGHT
500 PACIFIC AVE
SUITE 650
BREMERTON WA 98337

Attention:

THIS NUMBER MUST APPEAR
ON ALL INVOICES & INQUIRIES

Date: 08/09/24

Ship To: INFORMATION TECHNOLOGY
2930 Wetmore Ave, STE 6A
Everett, WA 98201 425-257-8776

Buyer: Daniel Trefethen 425-257-8905

LINE	QUANTITY	UNIT	DESCRIPTION	UNIT PRICE	AMOUNT
1	1	EA	Part #MDR for IoT Critical Insight	8,384.00	8384.00

ALL PRICING, TERMS AND CONDITIONS PER COOPERATIVE CONTRACT OMNIA PARTNERS #R200803. TO THE EXTENT THE TERMS AND CONDITIONS IN THIS PURCHASE ORDER ARE DIFFERENT THAN THE TERMS AND CONDITIONS OF THE COOPERATIVE CONTRACT, THE TERMS AND CONDITIONS MOST STRINGENT ON SUPPLIER SHALL APPLY. THE SUPPLIER CERTIFIES BY ACCEPTING THIS PURCHASE ORDER THAT TO THE BEST OF ITS KNOWLEDGE AND BELIEF THAT IT IS NOT PRESENTLY DEBARRED, SUSPENDED, PROPOSED FOR DEBARMENT, DECLARED INELIGIBLE, OR VOLUNTARILY EXCLUDED FROM COVERED TRANSACTIONS BY ANY FEDERAL DEPARTMENT.

SUBTOTAL 8,384.00
9.9 TAX 830.02

TOTAL 9,214.02

AUTHORIZED SIGNATURE:

City of Everett
Purchase Order (PO) Terms and Conditions

1. **ACCEPTANCE OF TERMS AND CONDITIONS.** Supplier shall provide the goods and/or services described in this PO in accordance with these terms and conditions unless otherwise noted on the face of the PO. Acceptance of this PO by either Supplier's written acknowledgment or commencement of performance shall create a binding contract and shall be conclusive evidence of Supplier's full acceptance of this PO and these terms and conditions. If this PO arises from an Invitation to Quote, Request for Proposals, or any other solicitation, then all provisions of such solicitation (including without limitation all specifications) are incorporated into these Terms and Conditions. If this PO arises from a cooperative contract, then all applicable provisions of the cooperative contract are incorporated into these Terms and Conditions. However, if there is a conflict between the provisions of these Terms and Conditions and the solicitation or cooperative contract, then the provision that is most stringent on Supplier and/or that grants the City greater rights shall control. If contract provisions are required by applicable federal, state, or local laws or regulations, then these Terms and Conditions are deemed to include such provisions. This PO expressly limits acceptance to the terms and conditions stated herein. All additional or different terms proposed by Supplier are objected to and hereby rejected unless otherwise provided in writing by the City's Procurement Manager or designee.
2. **AMENDMENT/CHANGES:** No change to this PO (including without limitation change to any term, condition, delivery, price, quality, quantity, or specification) will be effective without the written consent of the City's Procurement Manager or designee.
3. **TERMS AND CONDITIONS RELATED TO GOODS:**
 - a. **Handling:** No charges will be allowed for handling, which includes, but is not limited to, packing, wrapping, bags, containers, or reels unless otherwise stated herein. Material Safety Data Sheets must be included with shipments of any material requiring such documentation.
 - b. **Delivery Date:** For any change to the delivery date specified on this PO, Supplier shall give prior notification and obtain written approval thereto from the City's Procurement Manager or designee. With respect to delivery under this PO, time is of the essence, and this PO is subject to termination by the City for failure to deliver when specified. The acceptance by the City of late delivery with or without objection shall not waive the City's right to claim damages for such breach or constitute a waiver of timely performance of any Supplier obligation.
 - c. **Shipping Instructions:** Unless otherwise specified on this PO, all goods must be shipped prepaid, FOB Destination. Where shipping addresses indicate room numbers and/or inside delivery, the Supplier must make delivery to that location at no additional charge. Where specific authorization is granted to ship goods to FOB shipping point, Supplier must prepay all shipping charges and route as instructed or, if instructions are not provided, route by cheapest common carrier and provide the charge for such delivery as a separate item on Supplier's invoice. Each invoice for shipping charges shall contain the original or a copy of the bill indicating that the payment for shipping has been made. The City reserves the right to refuse COD shipments.
 - d. **Risk of Loss:** Regardless of FOB point, Supplier agrees to bear all risks of loss, injury, spoilation, or destruction of goods and materials ordered herein which occur prior to delivery. Such loss, injury, or destruction shall not release Supplier from any obligation hereunder.
 - e. **Free and Clear:** Supplier warrants that all goods delivered herein are free and clear of all liens, claims, or encumbrances of any kind.
 - f. **Identification:** All invoices, packing lists, packages, shipping notices, and other written documents relating to this PO shall contain the PO number. Packing lists shall be enclosed in each and every box or package shipped pursuant to this PO, indicating the contents therein.
 - g. **Rejection:** All goods purchased herein are subject to approval by the City. Any rejection of goods or materials resulting because of nonconformity to the terms and specifications of this PO, whether held by the City or returned to Supplier, will be at Supplier's risk and expense.
 - h. **Warranties:** Supplier warrants that goods are new, current, and fully warranted by the manufacturer. Delivered goods will comply with the PO and be free from defects in labor, material, and manufacture. All UCC implied and express warranties are incorporated in this PO. Supplier shall transfer all warranties to the City. Supplier warrants that goods supplied under this PO conform to the description and applicable specifications, shall be of good merchantable quality, and are fit for the purpose for which such goods are ordinarily employed, except that if a particular purpose is stated, the goods must then be fit for that particular purpose. This is in addition to any express warranties, standard warranty, and/or service guarantees given by Supplier. Supplier warrants that goods furnished on this PO do not infringe any patent, registered trademark, or copyright.
 - i. **Price:** If price is not stated on this PO, it is agreed that the goods shall be billed at the price last quoted or paid, or prevailing market price, whichever is lower.
4. **TERMS AND CONDITIONS RELATED TO SERVICES:**
 - a. **General:** Supplier shall perform the services described in this PO in a competent and professional manner. Without a written directive of an authorized representative of the City, Supplier shall not perform any services that are in addition to, or beyond the scope of, such services. If Supplier's proposal is attached to the PO, and if such proposal contains or incorporates any conditions or terms in addition to or different from the terms of this PO, then Supplier expressly agrees that such conditions or terms are neither incorporated nor included into this PO unless otherwise determined by the City's Procurement Manager or designee. Reports, drawings, plans, specifications, and any other intangible property created in furtherance of the services are property of the City for all purposes, whether the project for which they are made is executed or not, and may be used by the City for any purpose.
 - b. **Public Work:** If this PO is for construction or maintenance services or is otherwise for a public work, then (i) Supplier shall furnish all labor, tools, materials, equipment, and supplies required and shall, in a workmanlike manner, perform the work; (ii) Supplier shall comply with RCW 39.12 (Prevailing Wages), including without limitation Supplier submission of copies of "Statement of Intent to Pay Prevailing Wages" and "Affidavit of Wages Paid" to the City Clerk and Department of Labor and Industries; and (iii) Supplier agrees that the Supplier shall actively solicit the employment of minority group members. Supplier further agrees that the contractor shall actively solicit bids for the subcontracting of goods or services from qualified minority businesses. Supplier shall furnish evidence of the contractor's compliance with these requirements of minority employment and solicitation. Supplier further agrees to consider the grant of subcontracts to such minority bidders on the basis of substantially equal proposals in the light most favorable to such minority businesses. The Supplier shall be required to submit evidence of compliance with this section as part of the bid.
 - c. **Insurance:** Supplier shall procure and maintain insurance as required under insurance requirements at: <https://www.everettwa.gov/319/Procurement>.
5. **PAYMENT TERMS/TAXES/CASH DISCOUNT:** Unless otherwise stated on this PO, the terms of payment shall be net 30 days from receipt of a proper invoice. PO numbers must be noted on all invoices. Invoices will not be processed for payment until invoiced goods or services are received. Payments by the City are not assignable without the prior written consent of the City's Procurement Manager or designee. Unless otherwise provided in this PO, the City agrees to pay all State of Washington sales or use tax. No charge by Supplier shall be made for federal excise taxes, and the City agrees to furnish Supplier, upon acceptance of goods or services supplied under this order, with an exemption certificate. **In the event that the City is entitled to a cash discount, the period of computation will commence on the date of delivery or receipt of a correctly completed invoice, whichever is later. If an adjustment in payment is necessary due to damage, the cash discount period shall commence on the date final approval for payment is authorized. If a discount applies, but the invoice does not reflect the existence of a cash discount, the City is entitled to a cash discount with the period commencing on the date it is determined by the City that a cash discount applies.**
6. **COMPLIANCE WITH APPLICABLE LAWS/DISCRIMINATION:** Supplier shall comply with all applicable federal, state, local laws and regulations. Supplier shall possess and maintain all necessary licenses, permits, certificates, and credentials. If applicable, Supplier shall have a valid and current City of Everett business license. Supplier agrees not to discriminate against any employee or any other person in the performance of this PO because of race, creed, color, national origin, marital status, sex, age, disability, or other circumstances as may be defined by federal, state, or local law or ordinance.
7. **INDEMNIFICATION:** Supplier shall defend, indemnify, and hold the City, its officers, employees, and agents harmless from any and all claims, injuries, damages, losses, or suits, including attorney fees, resulting from the acts or omissions of Supplier, its contractors, agents or employees arising out of or in connection with the performance of this PO, except for injuries and damages caused by the sole negligence of the City. Should a court of competent jurisdiction determine that this PO is subject to RCW 4.24.115, then, in the event of liability for damages arising out of bodily injury to persons or damages to property caused by or resulting from the concurrent negligence of Supplier and the City, the Supplier's liability hereunder shall be only to the extent of Supplier's negligence. It is further specifically and expressly understood that the indemnification provided herein constitutes the Supplier's waiver of immunity under Industrial Insurance, Title 51 RCW, solely for the purpose of this indemnification. This waiver has been mutually negotiated by the parties. The provisions of this section shall survive the expiration or termination of this PO.
8. **TERMINATION:** The City may terminate this PO at any time with written notice to Supplier. Upon receipt of the written notice, Supplier shall stop performance, and City shall pay Supplier for goods and services delivered and accepted. If Supplier breaches any PO obligation or is declared insolvent, the City may terminate this PO for cause with written notice to Supplier, and Supplier shall be liable for all damages, including incidental and consequential damages, resulting from such breach.
9. **COOPERATIVE PURCHASING:** Agencies that have an Intergovernmental Cooperative Purchasing Agreement with the City may purchase from City contracts, including this PO, if so stated in the solicitation. The City is not responsible for any purchase order issued by another agency.
10. **OTHER:** The laws of the State of Washington govern this PO. Exclusive venue for any dispute relating to this PO shall be in Snohomish County Superior Court. Unless otherwise provided in this PO, this PO and all records associated with the PO are subject to public disclosure by the City without notice to Supplier. If a court of competent jurisdiction declares any provision of the PO to be invalid, the other provisions and the rights and obligations of the parties remain in effect. Any failure by the City to enforce strict performance of any provision of this PO will not constitute a waiver of the City's right to enforce such provision or any other provision of the PO. Supplier shall not assign, transfer, or encumber any rights, duties, or interests under this PO without the written consent of the City's Procurement Manager or designee.

Name: Kristal Matthews**Email:** kristal.matthews@criticalinsight.com**Phone:** +1 7148377488**Quote Date:** 08-09-2024**Quote Expiration:** 09-08-2024**Quote ID:** Q-17746-2**Bill To:****Name:** Chris Fadden**Company:** City of Everett, WA**Address:** 2930 Wetmore Ave., Ste. 6A,
Everett, WA, US, 98201**Phone:** 425-257-8600**Ship To:****Name:** Chris Fadden**Company:** City of Everett, WA**Address:** 2930 Wetmore Ave., Ste. 6A,
Everett, WA, US, 98201**Phone:** 425-257-8600**Contract Name:** OMNIA Partners - Cyber Security Solutions and Associated Products & Services**Contract #:** R200803**SERVICE SUBSCRIPTION**

SKU	Description	Duration	Qty	MO List Price	Disc %	MO Net Price
CI-P-IoT-4	MDR for IoT: Critical Insight performs MDR Services for pre-approved IoT environments.*	10	1	\$1,000.00	20%	\$800.00
One-time Setup	MDR Platform Setup Fee* ¹	1	1	\$480.00	20%	\$384.00

*Line items subject to Sales Tax and are not included in this quote.

¹Annual cost of these line items are billed on the Initial Invoice of each year they occur.³Internal Reference

Initial Invoice:	\$8,384.00
Total Contract Value:	\$8,384.00

TERMS AND CONDITIONS

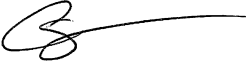
This Statement of Service ("SOS"), effective as of the date of the signature of the last party to sign (the "Effective Date") is subject to the Critical Insight Master Services Agreement dated 05-03-2023, the Critical Insight Description of Service attached here as Exhibit A, and any other Exhibits, Attachments or Amendments hereto, which are each incorporated herein by reference, and which together with this SOS constitute the "Agreement". Unless otherwise provided in this SOS, capitalized terms herein shall be as defined elsewhere in the Agreement. The terms of this Agreement constitute the final expression of the parties' binding understanding in respect to the subject matter hereof and supersede all prior or contemporaneous agreements, representations and understandings, written and oral, in respect to same. **Customer acknowledges that it has read the Agreement and agrees to be bound by its terms.**

- This Agreement will begin on the Effective Date and continue in effect for a period commencing on the Effective Date and terminating contemporaneous with the expiration or earlier termination of the Statement of Service and related Master Services Agreement, dated as of 07-19-2024.
- Billing shall be based on Critical Insight reporting. Critical Insight and Customer shall reconcile in good faith any discrepancies in their respective tracking records, provided Critical Insight's reporting shall control in the event of an irreconcilable discrepancy.
- Customer shall be invoiced on an annual basis in advance.
- The first invoice shall be issued thirty (30) days following the Effective Date.
- Payment of invoiced amounts due no later than thirty (30) calendar days from date of invoice.
- Pricing is based on the OMNIA Partners – Cyber Security Solutions and Associated Products & Services Contract #R200803.

Check one of the following:

- ☐ Purchase Order Required
☐ Purchase Order Not Required

**Customer
Signature**



Name Cassie Franklin

Title Mayor

Date 08/13/2024

**Critical Insight,
Inc.
Signature**


box SIGN 1V761766-4KYY9X63

Name Garrett Silver

Title CEO

Date Aug 9, 2024

**Billing Contact
Name**

Accounts Payable

**Billing Street
Address**

PO Box 12130

City, State, Zip

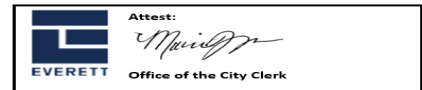
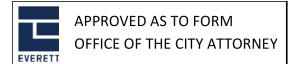
Everett, WA 98206

**Billing Contact
Phone**

425-257-8746

Billing Email

accountspayable@everettwa.gov



Internal Information

Affiliate: OMNIA

**EXHIBIT A
DESCRIPTION OF SERVICE**

CRITICAL INSIGHT ("CI") COMMERCIALY AVAILABLE PRODUCTS V. NOVEMBER 2023		
<u>SERVICE ID</u>	<u>SERVICE</u>	<u>RELEASE STATUS</u>
CI-P & CI-MDR	MDR: ON-PREMISES	GENERALLY AVAILABLE
	MDR: AWS	GENERALLY AVAILABLE
	MDR: O365 (FORMERLY MDR: MCAS)	GENERALLY AVAILABLE
	MDR: EDR	GENERALLY AVAILABLE
	MDR: MICROSOFT AZURE	GENERALLY AVAILABLE
	MDR: IOT	GENERALLY AVAILABLE
CI-CVI	ON-PREMISES VULNERABILITY SCANNING WITH NESSUS	GENERALLY AVAILABLE
CI-LR	ON-PREMISES LOG RETENTION	GENERALLY AVAILABLE

ALL COMMERCIALY AVAILABLE PRODUCTS & SERVICES OFFERED BY CI TO CUSTOMERS ARE DETAILED IN THIS DESCRIPTION OF SERVICES, SOME OF WHICH MAY NOT BE IN YOUR SUBSCRIPTION. **PLEASE SEE YOUR STATEMENT OF SERVICES FOR A LISTING OF THE SERVICES YOU HAVE PURCHASED.** "GENERALLY AVAILABLE" PRODUCTS & SERVICES ARE SUBJECT TO THE SERVICE LEVEL COMMITMENTS OR "SLA'S" SET FORTH ON PAGE 7 HEREOF. PRODUCTS & SERVICES LISTED AS "ALPHA" OR "BETA" ARE *NOT* SUBJECT TO ANY SLA'S. ALPHA/BETA PRODUCTS & SERVICES ARE PROVIDED 'AS IS' WITH NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. CI SHALL USE COMMERCIALY REASONABLE EFFORTS TO SUPPORT ALPHA AND BETA PRODUCTS & SERVICES ONLY ON AN 'AS AVAILABLE' BASIS.

SERVICE DESCRIPTION (SERVICE ID)	DESCRIPTION
CRITICAL INSIGHT PLATFORM (CI-P)	<p>THE PROVISIONING PROCESS TO SET UP THE INGEST CAPABILITIES FOR EACH ENVIRONMENT WILL BE ALIGNED TO THE MUTUALLY AGREED DATA STREAMS. THESE MUTUALLY AGREED DATA STREAMS ARE DOCUMENTED IN THE DATA INGEST LIST. CHANGES TO THE DATA INGEST LIST CAN OCCUR BASED UPON MUTUAL WRITTEN AGREEMENT (EMAIL SUFFICES) BETWEEN CI AND THE CUSTOMER. CI'S PRICING IS BASED ON THE ENVIRONMENTS THAT ARE MONITORED; ANY ADDITIONAL DATA STREAMS THAT INTRODUCE NEW ENVIRONMENTS MAY RESULT IN ADDITIONAL SUBSCRIPTION FEES.</p> <p>ENVIRONMENTS:</p> <ul style="list-style-type: none"> ON-PREMISES COLLECTOR(S) ("COLLECTOR")

	<ul style="list-style-type: none"> • O365 [FORMERLY MCAS] • ENDPOINT DETECTION & RESPONSE ("EDR") • AMAZON WEB SERVICES ("AWS") • MICROSOFT AZURE ("AZURE") • INTERNET OF THINGS / OPERATIONAL TECHNOLOGY ("IOT") <p>FOR ON PREMISES ENVIRONMENTS WITH COLLECTORS, CI WILL DELIVER AND INSTALL, OR PROVIDE INSTRUCTION FOR INSTALLATION OF, THE CI COLLECTOR ON CUSTOMER PREMISES AND VERIFY OPERATION.</p> <p>FOR ALL ENVIRONMENTS, CI WILL PROVIDE RELEVANT PROVISIONING INSTRUCTIONS FOR MONITORING TOOLS AND DATA STREAMS.</p> <p>DATA STREAMS: EACH ENVIRONMENT HAS UNIQUE DATA STREAMS AND CI WILL MONITOR ALL DATA STREAMS DOCUMENTED IN THE DATA INGEST LIST THROUGH APPROVED DATA INGESTION METHODS. THE FOLLOWING LIST DETAILS COMMON DATA STREAMS CI MONITORS PER ENVIRONMENT. THE DATA STREAMS CI WILL MONITOR FOR THE CUSTOMER ARE DOCUMENTED IN THIS DATA INGEST LIST:</p> <ul style="list-style-type: none"> • ON-PREMISES <ul style="list-style-type: none"> • SPECIFIC INTRUSION-DETECTION EVENT STREAMS • SPECIFIED DEVICE, SERVER, INFRASTRUCTURE, AND APPLICATION LOGS • CONTINUOUS ONSITE PACKET COLLECTION FOR NETWORK SEGMENTS SPECIFIED BY CUSTOMER <ul style="list-style-type: none"> • CI WILL GENERATE FLOW RECORDS FROM COLLECTED PACKETS • CI EPHEMERALLY STORES PACKETS FOR A PERIOD LIMITED BY THE STORAGE CAPACITY OF THE CUSTOMER'S CHOSEN COLLECTORS • AWS <ul style="list-style-type: none"> • GUARDDUTY ALERTS • CLOUDTRAIL LOGS • VPC FLOW RECORDS • O365 <ul style="list-style-type: none"> • SPECIFIC MICROSOFT DEFENDER FOR CLOUD APPS ALERT & EVENT STREAMS • SPECIFIC MICROSOFT DEFENDER FOR CLOUD APPS DISCOVERY ALERTS & EVENT STREAMS • Azure AD INTEGRATION FOR RAPID QUARANTINE ACTION AND USER ENRICHMENT • EDR <ul style="list-style-type: none"> • SPECIFIC SECURITY EVENT STREAMS DEPENDING ON APPROVED EDR • SPECIFIC ACTIONS DEPENDING ON APPROVED EDR • MICROSOFT AZURE <ul style="list-style-type: none"> • SPECIFIC MICROSOFT DEFENDER FOR CLOUD APPS ALERT & EVENT STREAMS • SPECIFIC MICROSOFT DEFENDER FOR CLOUD ALERT & EVENT STREAMS • SPECIFIC MICROSOFT AZURE AD IDENTITY PROTECTION ALERT & EVENT STREAMS • IOT
--	--

	<ul style="list-style-type: none"> SPECIFIC SECURITY EVENT STREAMS FOR ARMIS <p>SPECIFIC MICROSOFT AZURE AD IDENTITY PROTECTION ALERT & EVENT STREAMS SOME DATA STREAMS, SUCH AS SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) STREAMS OR EXTENDED DETECTION & RESPONSE (XDR) PRODUCTS WILL AGGREGATE DATA ACROSS MULTIPLE ENVIRONMENTS. CI WILL INCLUDE THE XDR OR SIEM PRODUCT AS AN ADDITIONAL DATA STREAM SO LONG AS IT IS AGGREGATING DATA STREAMS THAT ARE ALREADY DOCUMENTED IN THE DATA INGEST LIST.</p> <p>SOME DATA STREAMS INCLUDE FUNCTIONALITY THAT ENABLES CI TO PERFORM ACTIONS IN THE CUSTOMER ENVIRONMENT. IN CASES WHERE A DATA STREAM PROVIDES THIS FUNCTIONALITY, CI AND THE CUSTOMER WILL AGREE TO THE SCOPE AND ACTIONS THAT WILL BE TAKEN IN A SEPARATE DOCUMENT, I.E. RAPID QUARANTINE PLAYBOOK. CI WILL TAKE NO ACTION UNTIL THIS AGREEMENT IS DOCUMENTED IN WRITING.</p>
MANAGED DETECTION AND RESPONSE (CI-MDR)	<p>ACTIVATION:</p> <p>AN ENVIRONMENT WILL BE CONSIDERED ACTIVATED FOR MONITORING WHEN ALL SPECIFIED DATA STREAMS FOR AN ENVIRONMENT ARE ACTIVATED. FOR EACH DATA STREAM, CI WILL:</p> <ul style="list-style-type: none"> VERIFY CUSTOMER'S DATA STREAM IS CONFIGURED PER PROVISIONING INSTRUCTIONS WORK WITH CUSTOMER TO GENERATE TEST ALERTS WHERE POSSIBLE VERIFY TRANSMISSION OF ANY CUSTOMER DATA INTO CI'S CORPORATE ANALYSIS SYSTEMS, SOC DASHBOARDS AND TICKETING <p>CI MONITORS DELIVERY OF DATA STREAMS ON AN AUTOMATED BASIS AS AVAILABLE AND WILL ALSO PERFORM PERIODIC MANUAL REVIEWS.</p> <p>FOR DATA STREAMS THAT INCLUDE FUNCTIONALITY THAT ENABLES CI TO PERFORM ACTIONS IN THE CUSTOMER ENVIRONMENT, THE ACTIONS WILL BE ACTIVATED ONCE THE CUSTOMER AND CI AGREE IN WRITING AND THE ACTIONS ARE TESTED WITH THE CUSTOMER TO ENSURE OPERATIONAL READINESS.</p>
MANAGED DETECTION AND RESPONSE (CI-MDR)	<p>MONITORING:</p> <p>UPON THE SUCCESSFUL ACTIVATION OF SPECIFIED ENVIRONMENTS, CI WILL INGEST ANY APPROVED DATA STREAMS AND WILL ELEVATE ALERTS FROM THOSE STREAMS FOR REVIEW, AS APPROPRIATE. CI ANALYSTS REVIEW APPROVED DATA STREAMS FOR INDICATORS OF COMPROMISE WHICH INCLUDE BUT ARE NOT LIMITED TO:</p> <ul style="list-style-type: none"> ALERTS LINKED TO POOR REPUTATION IPS OR DOMAINS COMMAND AND CONTROL CONNECTIONS ANOMALOUS OR SUSPICIOUS ALERT PATTERNS SUDDEN SHIFTS IN THE VOLUME OF KEY ACTIVITIES EVENT CORRELATION WITH REGIONAL, SECTOR, OR GLOBAL CAMPAIGNS SELECTED EVENTS FROM 3RD PARTY SERVICES (SUCH AS 3RD PARTY EDR PRODUCTS, MICROSOFT PRODUCTS, AWS'S GUARDDUTY, ETC.)

	<p>FOR DATA STREAMS THAT INCLUDE FUNCTIONALITY THAT ENABLES CI TO TAKE ACTION IN THE CUSTOMER ENVIRONMENT, CI WILL WORK WITH THE CUSTOMER TO PERIODICALLY TEST ACTIONS TO ENSURE SERVICE QUALITY.</p>
<p>MANAGED DETECTION AND RESPONSE (CI-MDR)</p>	<p>RESPONSE:</p> <ul style="list-style-type: none"> • INVESTIGATION TICKET CREATED AND ASSIGNED TO CI ANALYST WITH A GOAL TO CONCLUDE THE INVESTIGATION WITHIN THE SPECIFIED SLA (<i>SEE SLA AGREEMENT</i>) • ANALYSTS INVESTIGATE AND ATTEMPT TO CONFIRM AN INCIDENT HAS OCCURRED BY ANALYZING RELEVANT AND AVAILABLE DATA <ul style="list-style-type: none"> • IN THE COLLECTOR ENVIRONMENT, “RELEVANT DATA” REFERS TO THE PACKET CAPTURE, NETWORK FLOWS AND SYSTEM LOGS FROM 30 SECONDS PRIOR TO UNTIL 30 SECONDS AFTER THE SUSPECT ACTIVITY IN STANDARD INVESTIGATIONS. WHEN WARRANTED, THE TIME PERIOD MAY EXPAND. • FOR ALL OTHER ENVIRONMENTS, RELEVANT AND AVAILABLE DATA REFERS TO ALL DATA THAT CI IS ABLE TO CAPTURE AND EFFECTIVELY MONITOR FROM THE APPROVED DATA STREAMS. • CONFIRMATION OCCURS WHEN EVIDENCE OF ATTACK OR COMPROMISE IS VERIFIED BY A CI ANALYST <p>TIERED RESPONSE:</p> <ul style="list-style-type: none"> • FOR ALL CONFIRMED INCIDENTS, NOTIFY CUSTOMER WITHIN THE SPECIFIED SLA (<i>SEE SLA AGREEMENT</i>) • FOR URGENT OR HIGH SEVERITY INCIDENTS, A FINAL INCIDENT ACTION PLAN WILL BE DELIVERED TO CUSTOMER AT THE TIME THAT ALL RELATED TICKETS ARE CLOSED. THE REPORT WILL INCLUDE: <ul style="list-style-type: none"> • SUMMARY OF INCIDENT • SUMMARY OF ANY CONFIRMED ACTIONS TAKEN (BY CI AND/OR CUSTOMER) • FINAL STATUS AND/OR RESOLUTION <p>RAPID QUARANTINE:</p> <ul style="list-style-type: none"> • IF CUSTOMER HAS A DATA STREAM THAT INCLUDE ACTIONS SUCH AS ISOLATING ENDPOINT, QUARANTINE ENDPOINT, OR BLOCK ACCOUNT, THE CUSTOMER CAN COMPLETE A RAPID QUARANTINE PLAYBOOK TO AUTHORIZE CI TO TAKE ADDITIONAL REMEDIATION ACTIONS. • CI WILL TAKE ACTION GOVERNED BY THE MUTUALLY AGREED RAPID QUARANTINE PLAYBOOK WHEN ANY INVESTIGATION REACHES THE THRESHOLDS DETERMINED IN THE PLAYBOOK. • ONCE AN INVESTIGATION REACHES THE THRESHOLDS, CI WILL EXECUTE ACTIONS DETAILED IN THE RAPID QUARANTINE PLAYBOOK WHICH MAY INCLUDE BUT ARE NOT LIMITED TO: <ul style="list-style-type: none"> • USE EDR TO QUARANTINE AN ENDPOINT • USE MICROSOFT AZURE ACTIVE DIRECTORY TO BLOCK AN ACCOUNT • REACH OUT TO CUSTOMER FOR APPROVAL TO QUARANTINE • NOTIFY CUSTOMER OF INCIDENT <p>MONTHLY ACTIVITY UPDATES:</p> <ul style="list-style-type: none"> • PUBLISHED MONTHLY <ul style="list-style-type: none"> • SECURITY INFORMATION RELEVANT TO THE ENVIRONMENT • INVESTIGATIONS COMPLETED • HIGH PRIORITY INVESTIGATIONS PERFORMED

CONTINUOUS VULNERABILITY IDENTIFICATION (CI-CVI)	<ul style="list-style-type: none"> • AUTOMATICALLY CONDUCTS INTERNAL NETWORK VULNERABILITY SCANS AT CUSTOMER-DEFINED FREQUENCIES AND IP SCOPES(S) • IDENTIFIES INSECURE CONFIGURATIONS, OPEN PORTS AND SERVICES, VULNERABLE SOFTWARE/SERVICE VERSIONS, AND MISSING PATCHES • GENERATES REPORTS WITH STEPS TO ELIMINATE EACH VULNERABILITY, AS WELL AS RISK VIA CVSS SCORES TO ALLOW PRIORITIZATION OF REMEDIATION EFFORTS • POPULATES A WEB DASHBOARD TO VIEW STATISTICS, VISUALIZATIONS, AND RESULTS <ul style="list-style-type: none"> • TABULAR RESULTS • GRAPHICAL REPRESENTATION OF TIME-BASED TRENDS FOR NEWLY IDENTIFIED VULNERABILITIES AND FOR REMEDIATED VULNERABILITIES
LOG RETENTION (CI-LR)	<ul style="list-style-type: none"> • DURING DEPLOYMENT CUSTOMER WILL PROVIDE CI WITH A LIST OF: <ul style="list-style-type: none"> • IN-SCOPE LOG SOURCES • STATIC IP OF THOSE LOG SOURCES • TIMEZONE OF THE LOG SOURCES • DURING DEPLOYMENT CUSTOMER WILL CONFIGURE THEIR LOG SOURCES TO SEND TO CI'S COLLECTOR AND CI WILL VERIFY SUCCESSFUL RECEPTION OF LOGS • THE SERVICE WILL BE ACTIVATED ONCE ALL IN-SCOPE LOG SOURCES ARE BEING RECEIVED SUCCESSFULLY BY CI'S CLOUD INFRASTRUCTURE • CI WILL STORE, HASH, AND ENCRYPT THE IN-SCOPE LOGS THROUGHOUT THE LIFETIME OF THE SERVICE • IT IS THE CUSTOMER'S RESPONSIBILITY TO SUCCESSFULLY TRANSFER THE LOGS ACCORDING TO CI'S DEPLOYMENT DOCUMENTATION • CUSTOMER CAN SUBMIT A REQUEST TO CI SUPPORT CONTAINING THE LOG, SOURCE, AND TIMEFRAME THEY WANT LOGS FROM • CI WILL PULL THE LOGS ACCORDING TO THE REQUEST & TIMEZONE ON RECORD AND SECURELY TRANSFER THE REQUESTED LOGS VIA CI'S FILE SHARE • UP TO 5 DATA REQUESTS AND UP TO 10% OF TOTAL STORED DATA CAN BE REQUESTED PER YEAR. MORE REQUESTS MAY BE SUBJECT TO A DATA OR PROFESSIONAL SERVICES FEE • AT THE END OF THE CONTRACT, CI WILL TRANSFER ALL STORED DATA BACK TO THE CUSTOMER AS PART OF THIS SERVICE

INCIDENT CLASSIFICATION FOR CRITICAL INSIGHT MDR

INCIDENT SEVERITY	DESCRIPTION
URGENT	<p>AN URGENT PRIORITY SECURITY INCIDENT IS A NETWORK EVENT OR SET OF NETWORK EVENTS THAT IS BELIEVED TO PRESENT A SERIOUS AND IMMEDIATE RISK TO THE CUSTOMER'S NETWORK ENVIRONMENT. CI WILL CONTACT THE CUSTOMER (CONTACT ON FILE) VIA PHONE AND EMAIL TO ATTEMPT RESOLUTION. EXAMPLES OF URGENT PRIORITY SECURITY INCIDENTS INCLUDE:</p> <ul style="list-style-type: none"> SUSPECTED ACCOUNT COMPROMISE WITH ACCOUNT MISUSE OBSERVED CUSTOMER SECURITY DEVICE HAS ALERTED CI TO A LIKELY COMPROMISE THAT HAS BEEN VERIFIED USING OTHER MDR DATA/TOOLS WITH NO EVIDENCE THE SECURITY DEVICE HAS MITIGATED THE INCIDENT SUSPECTED MALWARE INFECTION WITH EVIDENCE OF IMMEDIATE BUSINESS IMPACT COMMUNICATIONS OBSERVED WITH A SUSPECTED MALICIOUS HOST WITH EVIDENCE OF DATA EXFILTRATION OR IMMEDIATE BUSINESS IMPACT <p>REGULATED DATA SEEN UNENCRYPTED GOING TO AN EXTERNAL DESTINATION</p>
HIGH	<p>A HIGH PRIORITY SECURITY INCIDENT IS A NETWORK EVENT OR SET OF NETWORK EVENTS THAT IS BELIEVED TO PRESENT A RISK TO THE CLIENT'S NETWORK ENVIRONMENT. CI WILL CONTACT THE CUSTOMER (CONTACT ON FILE) VIA PHONE AND EMAIL TO ATTEMPT RESOLUTION. EXAMPLES OF HIGH PRIORITY SECURITY INCIDENTS INCLUDE:</p> <ul style="list-style-type: none"> SUSPECTED OR POTENTIAL ACCOUNT COMPROMISE WITH NO MISUSE OBSERVED SUSPECTED MALWARE INFECTION WITH EVIDENCE OF MALWARE SPREADING BUT NO EVIDENCE OF IMMEDIATE BUSINESS IMPACT SUSPECTED OR POTENTIAL SYSTEM COMPROMISE WITH NO EVIDENCE OF MISUSE REGULATED DATA SEEN UNENCRYPTED BETWEEN TWO INTERNAL HOSTS
MEDIUM	<p>A MEDIUM PRIORITY SECURITY INCIDENT IS A NETWORK EVENT OR SET OF NETWORK EVENTS THAT MAY BE A RISK TO THE CLIENT'S NETWORK ENVIRONMENT AND MAY INFORM FUTURE CUSTOMER ACTIONS. CI WILL CONTACT THE CUSTOMER (CONTACT ON FILE) VIA EMAIL TO ATTEMPT RESOLUTION. EXAMPLES OF MEDIUM PRIORITY SECURITY INCIDENTS INCLUDE:</p> <ul style="list-style-type: none"> ATTEMPTED ACCOUNT COMPROMISE WITH NO EVIDENCE OF SUCCESS SUSPECTED MALWARE INFECTION WITH NO EVIDENCE OF MALWARE SPREAD OR IMMEDIATE BUSINESS IMPACT
LOW	<p>A LOW PRIORITY SECURITY INCIDENT IS A NETWORK EVENT OR SET OF NETWORK EVENTS THAT IS NOT BELIEVED TO REPRESENT AN IMMEDIATE RISK TO THE CLIENT'S NETWORK ENVIRONMENT BUT DOES WARRANT AWARENESS AND INVESTIGATION. CI WILL CONTACT THE CUSTOMER (CONTACT ON FILE) VIA EMAIL TO ATTEMPT RESOLUTION. EXAMPLES OF LOW PRIORITY SECURITY INCIDENTS INCLUDE:</p> <ul style="list-style-type: none"> POTENTIALLY UNWANTED PROGRAM OBSERVED OTHER ISSUE THAT IS NOT AN IMMEDIATE SECURITY THREAT OBSERVED

SERVICE LEVEL AGREEMENT¹

CI PRODUCT	DESCRIPTION	SERVICE LEVEL	SLA CREDIT
CRITICAL INSIGHT PLATFORM <i>(CI-P)</i>	COLLECT, NORMALIZE, STORE, TRANSMIT, AND RETAIN SECURITY EVENT DATA	99.9% UPTIME IN A GIVEN MONTH FOR THE CI COLLECTOR WHILE CLIENT NETWORK IS FUNCTIONAL	2% OF MONTHLY FEE
	MAINTENANCE OF CI COLLECTOR	REPLACEMENT DEVICES SHIPPED WITHIN 3 BUSINESS DAYS OF FAILURE	2% OF MONTHLY FEE
MANAGED DETECTION AND RESPONSE <i>(CI-MDR)</i>	EVALUATE SECURITY ALERTS AND DETERMINE IF THEY ARE FALSE POSITIVES OR ACTUAL INCIDENTS	99% OF EVENTS ESCALATED TO ANALYST FOR REVIEW IN A GIVEN MONTH EVALUATED WITHIN 90 MINUTES	2% OF MONTHLY FEE
	INCIDENT REPORTING AND REMEDIATION FOLLOW-UPS	99% OF CONFIRMED INCIDENTS IN A GIVEN MONTH REPORTED TO CUSTOMER WITHIN 30 MINUTES OF CONFIRMATION	2% OF MONTHLY FEE
CONTINUOUS VULNERABILITY IDENTIFICATION <i>(CI-CVI)</i>	SCHEDULED VULNERABILITY SCANNING OF CUSTOMER NETWORK; REPORT UPLOAD OF SCAN RESULTS	AS VULNERABILITY SCANS COMPLETE, REPORT DATA UPLOADED TO CUSTOMER PORTAL OR DELIVERED TO CUSTOMER WITHIN 48 HOURS OF SCAN COMPLETION	2% OF MONTHLY FEE

- SERVICE LEVEL AGREEMENTS ONLY APPLY TO PRODUCTS & SERVICES IN GENERAL AVAILABILITY. ALPHA AND BETA PRODUCTS & SERVICES ARE NOT SUBJECT TO THIS SLA. PLEASE SEE PAGE 1 FOR A LIST OF PRODUCTS & SERVICES AND THEIR COMMERCIAL AVAILABILITY STATUS.*












Critical Insight MDR for IoT_8.12.2024_SD

Final Audit Report

2024-08-14

Created:	2024-08-12
By:	Marista Jorve (mjorve@everettwa.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAGFTcywjdyX3DuXALlaAWGa07M-5RRp1D

"Critical Insight MDR for IoT_8.12.2024_SD" History

-  Document created by Marista Jorve (mjorve@everettwa.gov)
2024-08-12 - 10:21:14 PM GMT
-  Document emailed to Chris Fadden (cfadden@everettwa.gov) for approval
2024-08-12 - 10:22:06 PM GMT
-  Email viewed by Chris Fadden (cfadden@everettwa.gov)
2024-08-13 - 6:13:10 AM GMT
-  Document approved by Chris Fadden (cfadden@everettwa.gov)
Approval Date: 2024-08-13 - 6:13:44 AM GMT - Time Source: server
-  Document emailed to Daniel Trefethen (DTrefethen@everettwa.gov) for approval
2024-08-13 - 6:13:46 AM GMT
-  Email viewed by Daniel Trefethen (DTrefethen@everettwa.gov)
2024-08-13 - 3:03:39 PM GMT
-  Document approved by Daniel Trefethen (DTrefethen@everettwa.gov)
Approval Date: 2024-08-13 - 3:03:59 PM GMT - Time Source: server
-  Document emailed to Tim Benedict (TBenedict@everettwa.gov) for approval
2024-08-13 - 3:04:02 PM GMT
-  Email viewed by Tim Benedict (TBenedict@everettwa.gov)
2024-08-13 - 3:10:12 PM GMT
-  Document approved by Tim Benedict (TBenedict@everettwa.gov)
Approval Date: 2024-08-13 - 3:10:48 PM GMT - Time Source: server
-  Document emailed to Cassie Franklin (cfranklin@everettwa.gov) for signature
2024-08-13 - 3:10:50 PM GMT

 Email viewed by Cassie Franklin (cfranklin@everettwa.gov)

2024-08-13 - 4:53:25 PM GMT

 Document e-signed by Cassie Franklin (cfranklin@everettwa.gov)

Signature Date: 2024-08-13 - 4:54:14 PM GMT - Time Source: server

 Document emailed to Marista Jorve (mjorve@everettwa.gov) for approval

2024-08-13 - 4:54:16 PM GMT

 Email viewed by Marista Jorve (mjorve@everettwa.gov)

2024-08-13 - 5:11:49 PM GMT

 Document approved by Marista Jorve (mjorve@everettwa.gov)

Approval Date: 2024-08-14 - 3:29:40 PM GMT - Time Source: server

 Agreement completed.

2024-08-14 - 3:29:40 PM GMT