Statement of Work

Managed Extended Detection and Response Proposal

Prepared for: 24-181 - UDT - City of Broken Arrow - Feb_May Proposal

Issued Date: 1/16/2024

Pricing and Signatures

City of Broken Arrow
220 S. First Street, Broken Arrow, OK 74012, US
Quote Expiration Date: 02/01/2024
Billing POC:
Billing Email:
Term Start Date: 02/01/2024
Term End Date: 05/31/2024
Node Count: 854

Module	Description	SKU	Monthly Price	Term	Ext. Price
MDR	24x7x365 managed extended detection and response services with dashboards and reporting	24-PS-MD-SO-XDR	$11,614.40	4	$46,457.60
				Total Investment	**$46,457.60**

One-time costs will be invoiced in advance upon signature of this proposal. Recurring fees shall be invoiced monthly in advance at the monthly rate set forth herein. On a quarterly basis, UDT will review node counts for devices and systems being monitored under this Order Form. If node counts increase greater than 10%, then pricing will be adjusted as a true up to reflect the new node counts.

The services being provided under this proposal will be performed pursuant and subject to the Terms and Conditions of Oklahoma State Contract OMES SW1050UDT.

Customer must meet and maintain all controls, provide evidence, and participate in shared controls throughout the term of this Agreement. This Agreement may be executed by the parties in counterparts which together shall constitute one and the same agreement among the parties. A facsimile signature shall constitute an original signature for all intent and purposes. The parties hereto have caused this Agreement to be executed by their respective duly authorized representatives as of the effective date hereof. Each party warrants and represents that its respective signatories, whose signatures appear below, have been and are on the date of signature duly authorized to execute this Agreement.

City of Broken Arrow	**UNITED DATA TECHNOLOGIES, INC.**
Name:	Name:
Title:	Title:
Signature:	Signature:
Date:	Date:

Product and Service Descriptions

MDR

Description
24x7x365 monitoring, detection, and response service with expert level engineering, development, maintenance, and administration support for Microsoft Sentinel SIEM.
SKUs:
24-PS-MD-SO-XDR
Inclusions:
1. As applicable, support CEF Forwarding onboarding with limitation (i.e. Palo Altos, Cisco ASAs) 2. Initial configuration Sentinel SIEM and log retention 3. Connecting EDR tools and data connectors to the SIEM with verification of proper data parsing, filtering, and posting of associated telemetry along with development of analytical detection rules 4. Verification of native Microsoft Sentinel integrations and 3rd party external data sources to the SIEM 5. Table Top Exercise (TTX) to validate Incident Response Plan 6. Ongoing deployment, validation, and tuning of analytic rules, playbooks, and workbooks into Sentinel SIEM. 7. Ongoing maintenance and tuning of existing analytics rules associated with 3rd party data sources 8. Ongoing expert level engineering, development, maintenance, and administration support for Microsoft Sentinel SIEM 9. Continuous monitoring of network traffic and security alerts across the endpoint detection and response tooling 10. Correlation and trend analysis, investigation, and documentation of events/incidents reported by ingested telemetry, Sentinel Analytics and machine learning (ML) 11. Daily health checks, log source monitoring, and rapid response to customer support requests. 12. Quarterly CRRs 13. Automated incident response containment of cyber security incidents via automated playbooks or manual intervention within deployed servers and endpoint devices hosted within, or AD joined with, the environment in response to security incidents. 14. SECOPS Module to provide security operations metrics and reporting 15. End-user support services,
Exclusions
1. The creation of custom data connectors that are not part of the Microsoft Content Hub 2. Recovery and restoration of servers, endpoint devices (i.e., restoration of backups, reimaging, cleanup of malware, etc.) 3. Defender for IoT Monitoring requires additional hardware and licensing 4. Forensic Services 5. Support for on-prem CEF forwarding infrastructure
Customer Requirements
1. Microsoft Azure Subscription 2. Sentinel Subscription 3. Customer Contact List 4. Provide Conquest global administration access 5. Site to site between on prem domain controls and Azure, if applicable 6. Dedicate a primary and alternate ARMED Administrator

Deliverables
1. Dashboard and reporting on operational KPIs, case metrics 2. Incident Response Plan 3. After Action Review Artifact

Appendix A: Terms and Conditions

This Master Subscription Agreement governs Conquest Cyber's provision of, and City of Broken Arrow's use of the Services in accordance with all appendices attached hereto.

If Customer registers for a free trial of Conquest Cyber's Services, the applicable provisions of this Agreement will also govern that free trial.

This Agreement incorporates all provisions in the Order Forms, Schedules, Exhibits, Supplements, Addendums, Amendments, and other documents that are referenced herein. All these documents taken together, including those effective in the future, shall constitute the entire agreement between Conquest Cyber and Customer and replace any prior oral and/or written communications, negotiations, and agreements relating to the subject matter hereof. This Agreement may not be altered supplemented or amended using other document(s) unless otherwise agreed to in a written agreement signed by both Parties.

DEFINITIONS

"Access Credentials" means any username, identification number, password, license or security key, security token, PIN, or other security code, method, technology, or device, used alone or in combination, to verify an individual's identity and authorization to access and use the Product and Services.

"Authorized Users" means Customer's employees, consultants, contractors, and agents (a) who are authorized by Customer to access and use the Services under the rights granted to Customer pursuant to this Agreement; and (b) for whom access to the Services has been purchased hereunder.

"Harmful Code" means any software, hardware, or other technology, device, or means, including any virus, worm, malware, or other malicious computer code, the purpose or effect of which is to (a) permit unauthorized access to, or to destroy, disrupt, disable, distort, or otherwise harm or impede in any manner any (i) computer, software, firmware, hardware, system, or network; or (ii) any application or function of any of the foregoing or the security, integrity, confidentiality, or use of any data Processed thereby; or (b) prevent Customer or any Authorized User from accessing or using the Services or Conquest Cyber Systems as intended by this Agreement. Harmful Code does not include any Conquest Cyber Disabling Device.

"Personal Information" means information that Customer provides or for which Customer provides access to Conquest Cyber, or information which Conquest Cyber creates or obtains on behalf of Customer, in accordance with this Agreement that: (i) directly or indirectly identifies an individual (including, but not limited to, for example, names, signatures, addresses, telephone numbers, email addresses, and other unique identifiers)]; or (ii) can be used to authenticate an individual (including, without limitation, employee identification numbers, government-issued identification numbers, passwords or PINs, user identification and account access credentials or passwords, financial account numbers, credit report information, student information, biometric, genetic, health, or health insurance data, answers to security questions, and other personal identifiers), in case of both subclauses (i) and (ii), including Sensitive Personal Information as defined herein). Customer's business contact information is not by itself Personal Information.

"Disabling Device" means any software, hardware, or other technology, device, or means (including any back door, time bomb, time out, drop dead device, software routine, or other disabling device) used by Conquest Cyber or its designee to disable Customer's use or any Authorized User's access to or use of the Services automatically with the passage of time or under the positive control of Conquest Cyber or its designee.

"Conquest Cyber Materials" means the Services, Specifications, Documentation, and Conquest Cyber Systems and any and all other information, data, documents, materials, works, and other content, devices, methods, processes, hardware, software, and other technologies and inventions, including any deliverables, technical or functional descriptions, requirements, plans, or reports, that are provided or used by Conquest Cyber or any Subcontractor in connection with the Services or otherwise comprise or relate to the Services or Conquest Cyber Systems. For the avoidance of doubt, Conquest Cyber Materials include Resultant Data and any information, data, or other content derived from Conquest Cyber's monitoring of Customer's access to or use of the Services, but do not include Customer Data.

"Conquest Cyber Personnel" means all individuals involved in the performance of Services as employees, agents, or independent contractors of Conquest Cyber or any Subcontractor.

"Conquest Cyber Systems" means the information technology infrastructure used by or on behalf of Conquest Cyber in performing the Services, including all computers, software, hardware, databases, electronic systems (including database management systems), and networks, whether operated directly by Conquest Cyber or through the use of third-party services.

"Services" means the Conquest proprietary Software such as ARMED ATK and services that are ordered by Customer under an Order Form, Statement of Work ("SOW"), or online purchasing portal, provided to Customer free of charge (as applicable) or under a free trial, and made available online by Conquest Cyber, including associated Conquest Cyber offline or mobile components, as described in the Conquest Cyber Materials. "Services" that are licensed or hosted by a third-party will be subject to that third-party's end user license agreement.

"Resultant Data" means data and information related to Customer's use of the Services that is used by Provider in an aggregate and anonymized manner, including compile statistical and performance information related to the provision and operation of the Services.

"Service Level Agreement (SLA)": means the agreement setting forth the Parties' objectives and the performance levels Conquest Cyber must meet for all included Services. The SLAs shall be governed by the terms and conditions of this MSA.

"Statement of Work (SOW)" means an order for Professional or Consulting Services, which has been completed and executed by both parties, and which specifies the scope and schedule of Professional Services to be performed by Conquest Cyber for Customer, and the applicable fees and such other terms as may be mutually agreed to. Each Statement of Work entered into by the Parties shall be governed by the terms and conditions of this Agreement.

"Third-Party Materials" means materials and information, in any form or medium, including any open-source or other software, documents, data, content, specifications, products, equipment, or components of or relating to the Services that are not proprietary to Provider.

1. SERVICES

1.1. Access and Use. Subject to and conditioned on Customer's and its Authorized Users' compliance with the terms and conditions of this Agreement, Conquest Cyber hereby grants Customer a non-exclusive, non-transferable (except in compliance with **Error! Bookmark not defined.**16.3) right to access and use the Services during the Term, solely for use by Authorized Users in accordance with the terms and conditions herein. Such use is limited to Customer's internal use.

1.2. Reservation of Rights. Nothing in this Agreement grants any right, title, or interest in or to (including any license) any Intellectual Property Rights in or relating to, the Services, Conquest Cyber Materials, or Third-Party Materials, whether expressly, by implication, estoppel, or otherwise. All rights, title, and interest in and to the Services, the Conquest Cyber Materials, and the Third-Party Materials are and will remain with Conquest Cyber and the respective rights holders in the Third-Party Materials.

1.3. Primary Point of Contact. Each party shall, throughout the Term, maintain within its organization an individual to serve as such party's primary point of contact for day-to-day communications, consultation, and decision-making regarding this Agreement. Each primary point of contact shall be responsible for providing all day-to-day consents and approvals on behalf of such party under this Agreement. Each party shall ensure its primary point of contact has the requisite organizational authority, skill, experience, and other qualifications to perform in such capacity. If either Party's Primary Point of Contact ceases to be employed by such party or such party otherwise wishes to replace its primary point of contact, such party shall promptly name a new point of contact by written notice to the other party.

1.4. ARMED ATK Administrator. Applicable to ARMED ATK subscriptions, Customer shall, throughout the Term, maintain within its organization an individual to serve as the Customer's ARMED ATK administrator who will administer the Customer's ARMED ATK software instance for the Customer's organization. Administration of the ARMED ATK software includes, but is not limited to, meeting with Conquest Cyber's Business Resiliency Delivery team on an agreed to cadence by the Parties, to help work through the NIST CSF Cyber Security Framework recommended best practices and Customer's desired maturity, and working through any action items as outlined and directed in the ARMED ATK software.

1.5. Changes. Conquest Cyber reserves the right, in its sole discretion, to make any changes to the Services and Conquest Cyber Materials that it deems necessary or useful to: (a) maintain or enhance: (i) the quality or delivery of Conquest Cyber's Services; or (ii) the Services' cost efficiency or performance; or (b) to comply with applicable law. Without limiting the foregoing, either party may, at any time during the Term, request in writing changes to the Services. The Parties shall evaluate and, if agreed, implement all such requested changes in accordance with the change procedure set forth in Section 4.

1.6. Subcontractors. Conquest Cyber may from time to time in its discretion engage third parties to perform Services (each, a "Subcontractor").

1.7. Suspension or Termination of Services. Provider may, directly or indirectly, and by use of a Conquest Cyber Disabling Device or any other lawful means, suspend, terminate, or otherwise deny Customer's, any Authorized User's, or any other Person's access to or use of all or any part of the Services or Provider Materials, without incurring any resulting obligation or liability, if: (a) Conquest Cyber receives a judicial or other governmental demand or order, subpoena, or law enforcement request that expressly or by reasonable implication requires Conquest Cyber to do so; or (b) Conquest Cyber believes, in its reasonable discretion, that: (i) Customer or any Authorized User has failed to comply with any material term of this Agreement, or accessed or used the Services beyond the scope of the rights granted or for a purpose not authorized under this Agreement or in any manner that does not comply with any instruction or requirement of the Specifications; (ii) Customer or any Authorized User is, has been, or is likely to be involved in any fraudulent, misleading, or unlawful activities [relating to or in connection with any of the Services]; or (iii) this Agreement expires or is terminated in accordance with the termination terms set forth in this Agreement. This Section 1.7 does not limit any of Provider's other rights or remedies, whether at law, in equity, or under this Agreement.

2. TERM AND TERMINATION

2.1. Term and Renewal. This Agreement commences on the date the first Order Form is signed by the Customer and shall continue until all subscribed Order Forms have expired or been terminated. The term of each subscription shall be as specified in the applicable Order Form ("Subscription Term"). Unless specified otherwise in an Order Form, upon expiration of each Subscription Term, the Subscriptions shall automatically renew for one (1) year terms unless either party gives the other party written notice ninety (90) days prior to the expiration of any renewal Term of its desire not to renew same, or this Agreement is earlier terminated in accordance with the terms of this Agreement. Order Form terms and payment obligations are non-cancelable, and fees paid are non-refundable.

2.2. Termination. This Agreement and any Order Form may be terminated by either party if the other party breaches any of its material obligations under this Agreement and fails to cure such breach within thirty (30) days after receipt of written notice of such breach. However, termination of this Agreement will not affect Customer's obligation to make payments for Services provided prior to the date of termination. Notwithstanding anything in this Agreement to the contrary, Conquest Cyber may immediately terminate this Agreement and/or any Schedule in whole or in part if: (i) Customer fails to comply with the payment provisions of this Agreement and such failure continues more than thirty (30) days after Conquest Cyber's delivery of written notice thereof; (ii) upon the insolvency, bankruptcy, or dissolution of Customer; (iii) if Customer makes or seeks to make a general assignment for the benefit of its creditors;

2.3. Effect of Termination or Expiration. Upon any expiration or termination of this Agreement, except as expressly otherwise provided in this Agreement:

2.3.1. All rights, licenses, consents, and authorizations granted by either party to the other hereunder will immediately terminate;

2.3.2. Conquest Cyber shall immediately cease all use of any Customer Data or Customer's Confidential Information and (i) promptly within thirty (30) days return to Customer, or at Customer's written request destroy, all documents and tangible materials containing, reflecting, incorporating, or based on Customer Data or Customer's Confidential Information; and (ii) permanently erase all Customer Data and Customer's Confidential Information from all systems Provider directly or indirectly controls[, provided that, for clarity, Provider's obligations under this Section 14.4(b) do not apply to any Resultant Data.

2.3.3. Customer shall immediately cease all use of any Services or Conquest Cyber Materials and (i) promptly within thirty (30) days return to Conquest Cyber, or at Conquest Cyber's written request destroy, all documents and tangible materials containing, reflecting, incorporating, or based on any Conquest Cyber Materials or Conquest Cyber's confidential information; and (ii) permanently erase all Conquest Cyber Materials and Conquest Cyber's Confidential Information from all systems Customer directly or indirectly controls.

3. FEES AND PAYMENT TERMS

3.1. Fees. The Services will be invoiced annually in advance at the rates set forth in the applicable Order Form. Except as otherwise specified in an Order Form, (i) fees are based on Services subscriptions purchased and not actual usage, and (ii) Order Form terms and payment obligations are non-cancelable, and fees paid are non-refundable.

3.2. Payment Terms. All invoices are due and payable net thirty (30) days from the date of invoice. Conquest Cyber reserves the right to charge Customer a late penalty of 1.5% per month applied against undisputed overdue amounts, or the maximum rate permitted by law, whichever is less. Late penalties will be recalculated every 30 days thereafter based on Customer's then-current outstanding balance. In addition, Conquest Cyber, without waiving any other rights or remedies to which it may be entitled, shall have the right to suspend or terminate any or all Services and refuse additional Order Forms and Change Request Orders until Conquest Cyber's receipt of all overdue amounts. Conquest Cyber shall have no liability to Customer for any such suspension or termination of the Services or for its refusal of additional Change Request Orders. Conquest Cyber further reserves the right to seek collection of all overdue amounts (including by referral to third party collectors), plus all reasonable fees (including reasonable attorneys' fees) and costs associated with such collection. Notwithstanding the foregoing, Conquest Cyber will not exercise its rights under this clause for overdue charges if Customer is disputing the applicable charges reasonably and in good faith and is cooperating diligently to resolve the dispute.

3.3. Taxes. All Fees and other amounts payable by Customer under this Agreement are exclusive of taxes and similar assessments. Without limiting the foregoing, Customer is responsible for all sales, use, and excise taxes, and any other similar taxes, duties, and charges of any kind imposed by any federal, state, or local governmental or regulatory authority on any amounts payable by Customer hereunder, other than any taxes imposed on Conquest Cyber's income.

3.4. No Deductions or Setoffs. All amounts payable to Conquest Cyber under this Agreement shall be paid by Customer or Conquest Cyber in full without any setoff, recoupment, counterclaim, deduction, debit, or withholding for any reason (other than Service Credits issued pursuant to the Service Level Agreement included herein as Exhibit B).

4. ORDER FORM AND MODIFICATIONS

4.1. Order Forms. This Agreement shall govern each Order Form and/or Statement of Work and Customer will be responsible for any purchases under this Agreement. If the Customer wishes to add or change Services, Customer shall complete a written statement that references the objective, scope of service requested, and deliverable requirements (the "Change Order Process"). All Services obtained under this Agreement are subject to credit and credit terms as determined solely by Conquest Cyber.

4.2. Changing or Modifying Statements of Work or an Order Form. If the parties wish to change or modify an existing Order Form or Statement of Work, they shall execute a written statement that references the specific Order Form or Statement of Work by date, purchase order number, or other identifier, and describes the requested changes using the Change Order Process. No changes to an Order Form and/or Statement of Work shall become effective until both parties have mutually agreed upon and executed the Change Order.

4.3. Order of Precedence of Documents. In the event of a conflict between the documents that constitute the Agreement, the documents shall govern in the following order of precedence: (i) the Agreement; (ii) the Order Form; and (iii) applicable provisions in the Conquest Cyber Materials.

5. USE RESTRICTIONS; SERVICE USAGE AND DATA STORAGE

5.1. Subscriptions. Unless otherwise provided in the applicable Order Form, purchased Services are purchased as subscriptions for the term stated in the Order Form. Any added subscriptions shall be subject to a new Order Form.

5.2. Use Restrictions. Customer shall not, and shall not permit any other person to, access or use the Services or the Conquest Cyber Materials except as expressly permitted by this Agreement and, in the case of Third-Party Materials, the applicable third-party license agreement. For purposes of clarity and without limiting the generality of the foregoing, Customer shall not, except as this Agreement expressly permits:

5.2.1. Copy, modify, or create derivative works or improvements of the Services or Conquest Cyber Materials;

5.2.2. Rent, lease, lend, sell, sublicenses, assign, distribute, publish, transfer, or otherwise make available any Services or Conquest Cyber Materials to any person, including on or in connection with the internet or any time-sharing, service bureau, software as a service, cloud, or other technology or service.

5.2.3. Reverse engineer, disassemble, decompile, decode, adapt, or otherwise attempt to derive or gain access to the source code of the Services or Conquest Cyber Materials, in whole or in part;

5.2.4. Bypass or breach any security device or protection used by the Services or Conquest Materials or access or use the Services or Conquest Materials other than by an Authorized User through the use of his or her own valid Access Credentials;

5.2.5. Input, upload, transmit, or otherwise provide to or through the Services or Provider Systems, any information or materials that are unlawful or injurious, or contain, transmit, or activate any Harmful Code;

5.2.6. Damage, destroy, disrupt, disable, impair, interfere with, or otherwise impede or harm in any manner the Services, Conquest Systems, or Conquest's provision of services to any third party, in whole or in part;

5.2.7. Remove, delete, alter, or obscure any trademarks, Specifications, Documentation, EULA, warranties, or disclaimers, or any copyright, trademark, patent, or other intellectual property or proprietary rights notices from any Services or Provider Materials, including any copy thereof

5.2.8. Access or use the Services or Conquest Cyber Materials in any manner or for any purpose that infringes, misappropriates, or otherwise violates any Intellectual Property Right or other right of any third party, or that violates any applicable law;

5.2.9. Access or use the Services or Conquest Cyber Materials for purposes of competitive analysis of the Services or Conquest Cyber Materials, the development, provision, or use of a competing software service or product or any other purpose that is to Conquest Cyber's detriment or commercial disadvantage;

5.2.10. Otherwise access or use the Services or Conquest Cyber Materials beyond the scope of the authorization granted under this Section 5.

6. CUSTOMER OBLIGATIONS

6.1. Customer Systems and Cooperation. Customer shall at all times during the Term: (a) set up, maintain, and operate in good repair and in accordance with the Conquest Cyber Materials and instructions all Customer Systems on or through which the Services are accessed or used; (b) provide Conquest Cyber Personnel with such access to Customer's premises and Customer's Systems as is necessary for Conquest Cyber to perform the Services in accordance with the Service Level Agreement ("SLA"); and (c) provide all cooperation and assistance as Conquest Cyber may reasonably request to enable Conquest Cyber to exercise its rights and perform its obligations under and in connection with this Agreement.

6.2. Feedback. Customer shall provide prompt feedback (including, without limitation, any enhancements, improvements, modifications, bug fixes and identification of potential errors) to Conquest Cyber regarding the operation or use of the Services when it is requested, which may include, among other things, filing online reports, participating in telephone interviews, maintaining a record of problems or errors, providing suggestions and ideas and responding to written surveys that may be provided by Conquest Cyber (collectively,

"Feedback"). Customer hereby assigns to Conquest Cyber any and all right, title and interest in and to Feedback, including, without limitation, any and all intellectual property rights therein and goodwill with respect thereto. Accordingly, Customer acknowledges and agrees that Conquest Cyber may use, disclose, reproduce, license, distribute and otherwise commercialize Feedback.

6.3. Effect of Customer Failure or Delay. Conquest Cyber is not responsible or liable for any delay or failure of performance caused in whole or in part by Customer's delay in performing, or failure to perform, any of its obligations under this Agreement (each, a "Customer Failure").

6.4. Corrective Action and Notice. If Customer becomes aware of any actual or threatened activity prohibited by **Error! Bookmark not defined.**5, Customer
shall, and shall cause its Authorized Users to, immediately: (a) take all reasonable and lawful measures within their respective control that are necessary to stop the activity or threatened activity and to mitigate its effects (including, where applicable, by discontinuing and preventing any unauthorized access to the Services and Provider Materials and permanently erasing from their systems and destroying any data to which any of them have gained unauthorized access); and (b) notify Provider of any such actual or threatened activity.

6.5. Non-Solicitation. During the Term and for one (1) year after, Customer shall not, and shall not assist any other Person to, directly or indirectly, recruit or solicit (other than by general advertisement not directed specifically to any Person or Persons) for employment or engagement as an independent contractor any Person then or within the prior twelve (12) months employed or engaged by Conquest Cyber or any Subcontractor and involved in any respect with the services or performance of this Agreement.

7. MODIFICATION/DISCONTINUATION/MAINTENANCE

7.1. Modification to or Discontinuation of the Service. Conquest Cyber reserves the right at any time and from time to time to modify, temporarily or permanently, the Service (or any part thereof), provided such modification does not diminish the functionality of the Service to the Customer on which the Customer materially relies. Notwithstanding the foregoing, except for routinely scheduled down time, or as otherwise provided in this Agreement, Conquest Cyber shall use commercially reasonable efforts to notify Customer prior to any such modification.

7.2. Maintenance. In order to perform maintenance, including infrastructure and application upgrades, there will be routinely scheduled down time. Conquest Cyber further reserves the right on approximately a quarterly basis to issue new releases in which Conquest Cyber adds functionality to the Service. Customer acknowledges that these periodic major releases can take several hours to complete. The time necessary to provide such periodic releases shall not be counted in any service level or availability calculations. Conquest Cyber shall consult with the Customer and, unless otherwise agreed upon, shall install such major releases during routinely scheduled down time as set forth above. Customer shall be apprised of software upgrades and or patch releases to the Service. In the event of a patch release, a full IQ validation may not be undertaken. It shall be the Customer's responsibility to perform any required UAT/PQ validation. In the event that Conquest Cyber, in its sole discretion, determines that any unscheduled maintenance is necessary, Conquest Cyber will use commercially reasonable efforts to notify Customer as soon as it becomes aware of such need.

8. INDEMNIFICATION

8.1. General Indemnification. Each party shall defend the other party and each of its members, directors, officers, employees, parents, and affiliates (collectively referred to in this Section as "Indemnitees"), harmless from and against any claims, causes of action, suits of any nature, liabilities, reasonable settlements, losses, damages, costs and expenses (including reasonable attorneys' fees) on account of unaffiliated third-party claims based on the indemnifying party's gross negligence or intentional misconduct, and indemnify each Indemnitee on account of all resulting losses, damages, costs, and expenses (including reasonable attorneys' fees) finally awarded to the third-party by a court of competent jurisdiction (or an arbitration panel or other tribunal, as applicable) or pursuant to a settlement agreement. The indemnifying party may settle, at its sole expense, any claim for which it is responsible under this Section provided that the terms of the settlement do require payment by, do not admit any fault or liability of, and do not impose any restrictions or otherwise enjoin any acts by the indemnified party. The indemnifying party shall control the defense and/or settlement of any claim covered by this Section, provided that the indemnified party reserves the right to employ counsel at its own expense and participate in the defense.

8.2. Intellectual Property Indemnification. Conquest Cyber will indemnify, defend and hold harmless Customer for losses Customer incurs as a direct result of any unaffiliated third party claim based on any claim that the Service infringes any U.S. copyright, trademark or trade secret, except to the extent resulting from (i) Customer's modification of the Service or combination by Customer of the Services with other products or services if the Service would not have been infringing but for such combination or modification, (ii) Customer's use of the Service in a manner not authorized herein or for which it was not designed, (iii) Customer's failure to use an updated non-infringing version of the applicable intellectual property to the extent Customer was notified that the update cured an infringement, (iv) changes to the Service made by Conquest Cyber at the direction of the Customer or (v) Customer Data. If any item for which Conquest Cyber has an indemnification obligation under this Section becomes, or in Conquest Cyber's reasonable opinion is likely to become, the subject of an infringement or misappropriation claim or proceeding, Conquest Cyber will, in addition to indemnifying Customer as provided in this Section, promptly take the following actions, at no additional charge to Customer, in the listed order of priority: (a) secure the right to continue using the item or (b) replace or modify the item to make it non-infringing. If neither of such actions can be accomplished by Conquest Cyber using commercially reasonable efforts, and only in such event, Conquest Cyber will remove the item from the Service and the applicable Service fee will be equitably adjusted to reflect such removal. This Section

8.2 states Customer's sole and exclusive remedy for Conquest Cyber's infringement or misappropriation of intellectual property of a third party.

9. REPRESENTATIONS AND WARRANTIES

9.1. Customer Representations. Customer hereby represents and warrants the following:

9.1.1. Customer provided content is accurate, and belongs to Customer (or is licensed by Customer), and Customer has the power and authority to allow Conquest Cyber to use the Customer provided information as described in this Agreement or relevant Order Form

9.1.2. Customer shall not use the Services for any illegal purpose, or in any manner that infringes or tends to infringe the rights of any third parties; and

9.1.3. Customer has the power and authority to enter into, and be bound by, the terms of this Agreement.

9.2. Warranty of Functionality. Conquest Cyber warrants to Customer during the Term of this Agreement that the Service will comply with the material functionality described in the Order Form and Conquest Cyber Materials and that such functionality will be maintained in all material respects in subsequent upgrades to the Service. Customer's sole and exclusive remedy for Conquest Cyber's breach of this warranty shall be that Conquest Cyber shall use commercially reasonable efforts to correct such errors or modify the Service to achieve the material functionality described in the Order Form and Conquest Cyber Materials within a reasonable period of time.

9.3. Disclaimer of Warranties. CONQUEST CYBER ADOPTS ALL NECESSARY MEASURES SO THE INFORMATION PROVIDED AS PART OF THE SERVICES IS OF SUFFICIENT QUALITY AND FROM SOURCES CONQUEST CYBER CONSIDERS TO BE RELIABLE, INCLUDING, WHEN APPROPRIATE, INDEPENDENT THIRD-PARTY SOURCES. CUSTOMER UNDERSTANDS AND ACKNOWLEDGES THAT CONQUEST CYBER IS NOT AN AUDITOR AND CANNOT IN EVERY INSTANCE INDEPENDENTLY VERIFY OR VALIDATE INFORMATION RECEIVED AS PART OF THE SERVICES. CONQUEST CYBER IS NOT RESPONSIBLE FOR CUSTOMER'S FAILURE TO ADHERE AND COMPLY WITH CONQUEST CYBER RECOMMENDATIONS AND REGULATORY CONTROLS IMPLEMENTED AS PART OF THE SERVICES. THE SERVICES TO BE DELIVERED UNDER THIS AGREEMENT ARE NEITHER INTENDED NOR GUARANTEED TO ACHIEVE THE IMPOSSIBLE GOAL OF RISK ELIMINATION, AND CONQUEST CYBER EXPRESSLY DISCLAIMS ANY SUCH INTENT OR GUARANTEE. CONQUEST CYBER MAKES NO REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, TO CUSTOMER OR ANY OTHER PERSON OR ENTITY AS TO THE ACCURACY, RESULTS, TIMELINESS, COMPLETENESS, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE WITH RESPECT TO THE SERVICES OR ANY RELATED MATERIALS.

10. LIMITATION OF LIABILITY

10.1. TO THE FULLEST EXTENT POSSIBLE UNDER APPLICABLE LAW, NEITHER PARTY (NOR ITS EMPLOYEES, AGENTS, SUPPLIERS OR AFFILIATES) SHALL BE LIABLE TO THE OTHER FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL LOSS OR DAMAGE OF ANY KIND, INCLUDING WITHOUT LIMITATION ARISING IN CONNECTION WITH THE AGREEMENT, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, EVEN IF THE PARTY HAS BEEN ADVISED OR SHOULD BE AWARE OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL CONQUEST CYBER (OR ITS EMPLOYEES, AGENTS, SUPPLIERS, MEMBERS OR AFFILIATES) BE LIABLE FOR (A) ANY LOST PROFITS, REVENUE, SALES,SAVINGS, OR VALUE, (B) LOSS OF DATA OR INABILITY TO ACCESS DATA, OR (C) ANY DAMAGES INCURRED BY ANY THIRD PARTY AS A RESULT OF A SECURITY BREACH OF CUSTOMER'S NETWORK, UNLESS SUCH DAMAGES WERE INCURRED BY A THIRD PARTY AS A RESULT OF CONQUEST CYBER'S GROSS NEGLIGENCE OR INTENTIONAL MISCONDUCT.

10.2. EXCEPT FOR CLAIMS ARISING FROM A PARTY'S BREACH OF ITS CONFIDENTIALITY OBLIGATIONS UNDER THIS AGREEMENT, BREACH OF CONQUEST CYBER'S OR A THIRD-PARTY'S INTELLECTUAL PROPERTY RIGHTS UNDER THIS AGREEMENT, EACH PARTY'S ENTIRE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER ARISING UNDER OR RELATED TO BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, OR ANY OTHER LEGAL OR EQUITABLE THEORY SHALL BE LIMITED TO THE AMOUNTS PAID OR PAYABLE UNDER THE ORDER FORM WHERE THE CLAIM AROSE IN THE THREE (3) MONTH PERIOD PRIOR TO THE DATE THE CLAIM.

10.3. TO THE FULLEST EXTENT PERMITTED BY LAW, IT BEING THE INTENT OF THE PARTIES FOR ANY APPLICABLE PROVISIONS OF THIS AGREEMENT TO BE ENFORCEABLE AS BETWEEN THE PARTIES, EACH PARTY WAIVES COMPLIANCE BY THE OTHER PARTY WITH ANY APPLICABLE LAWS, RULES, OR REGULATIONS REGARDING THE CONSPICUOUSNESS OF ANY APPLICABLE PROVISIONS HEREOF, INCLUDING REQUIREMENTS REGARDING FONT SIZE, CAPITALIZATION, BOLD AND/OR ITALICIZED TEXT, OR ANY OTHER SPECIFIED REQUIREMENTS, WHETHER OR NOT OF A SIMILAR KIND OR NATURE TO ANY OF THE FOREGOING. NOTHING HEREIN SHALL PREVENT EITHER PARTY FROM OBTAINING INJUNCTIVE RELIEF.

11. INSURANCE

11.1. At all times during the terms of this Agreement, Conquest shall procure and maintain, at its sole cost and expense, at least the following types and amounts of insurance coverage:

11.1.1. Commercial General Liability with limits no less than $1,000,000 per occurrence and $2,000,000 in the aggregate including bodily injury and property damage and products and completed operations and advertising liability, which policy will include contractual liability coverage insuring the activities of Conquest under this Agreement;

11.1.2. Worker's Compensation with limits no less than the minimum amount required by applicable law; and

11.1.3. Errors and Omissions/Professional Liability with limits no less than $1,000,000 per occurrence and $2,000,000 in the aggregate.

11.2. All insurance policies required pursuant to Section 11.1 shall: (a) be issued by an insurance company with an A- rating or higher; (b) provide that such insurance carriers give Customer at least 30 days' prior written notice of cancellation or non-renewals of policy coverage; provided that, prior to such cancellation, Conquest shall have new insurance policies in place that meet the requirement of Section 11.1; (c) waive any right of subrogation of the insurers against Customer; (d) provide that such insurance be primary insurance and any similar insurance in the name of and/or for the benefit of Customer shall be excess and non-contributory; and (e) name Customer as additional insureds.

11.3. Upon the written request of Customer, Conquest shall provide Customer with copies of the certificates of insurance for all insurance coverage required by Section 11.1. Section 11.1 shall not be construed in any manner as waiving, restricting or limiting the liability of either party for any obligations imposed under this Agreement (including, but not limited to, any provisions requiring a party hereto to indemnify, defend and hold the other harmless under this Agreement).

12. SUPPORT AND SECURITY

12.1. Conquest Cyber's Access to Secure Information Systems and Data. Unless otherwise expressly provided in an Order form, Conquest Cyber is not responsible for any information stored or transferred via the Services, for backing up or maintaining copies of any data (including, without limitation, Customer Data, or for the removal or disposal of any confidential, proprietary, or personal information. Conquest Cyber shall not attempt to access Customer secure network(s) or other information systems without Customer prior consent, either via its personnel performing Services onsite, or remotely. To the extent reasonably required for the provision of the Services, Customer hereby grants Conquest Cyber the right to use Customer Data subject to Sections 12 hereunder.

13. CONFIDENTIALITY

13.1. The following information is "Confidential Information": (i) as to both parties, the terms of this Agreement, and all information exchanged by the parties during negotiations culminating in this Agreement and during the Term of this Agreement, any information related to a party's performance of, or failure to perform, this Agreement, and any information that is marked or designated as "Confidential" or with like notice; (ii) as to the party disclosing the information, any information related to that party's assets, liabilities, financial results, financing plans, business strategies, product development plans, operations, source code, technology, know-how, trade secrets, Customers, Conquest Cyber, contractors, personnel, and all other information that a reasonable person would understand to be confidential; and (iii) as to Customer, data center locations, data center designs (including non-graphic information observed at Customer data center), Customer Data but excluding in all cases any information which is independently developed by the other party as shown by such party's written business records, or information that becomes generally available to the public other than through breach of this Agreement, or violation of law or other agreement. Each party agrees not to disclose the other party's Confidential Information to any third party except to its agents and representatives who need to know the information to represent or advise it with respect to the subject matter of this Agreement and who are bound by written non-disclosure obligations at least as stringent as those stated in this Agreement; provided, however, that a party will not be liable for disclosure of the other party's Confidential Information if it is required by law or regulation to be disclosed and the disclosing party gives advance written notice of the disclosure to the other party at the earliest possible time, or the party discloses the information as part of a bona fide legal proceeding to enforce its rights under this Agreement. Each party agrees to use at least a reasonable degree of care to protect the other party's Confidential Information. Each party agrees not to use the other party's Confidential Information except in connection with the performance of its obligations or exercise of its rights under this Agreement.

13.2. Each party shall return or destroy the other party's Confidential Information on completion of the Services, or earlier on request of the other party, provided that a party may retain the other party's Confidential Information in backup medium where return or deletion is not commercially reasonable, or otherwise as required by law. On request of a party, an officer of the other party shall certify its compliance with the preceding sentence.

14. FORCE MAJEURE

14.1. Neither party shall be responsible for a delay in its respective performance under this Agreement, other than a delay in payment for Services already performed, if such delay is caused by circumstances, events or contingencies, existing or future, beyond the reasonable control of the claiming party, including "acts of God," abnormal weather conditions or other natural catastrophes, war (whether declared or not), terrorism, sabotage, computer viruses, riots, strikes, lockouts or other industrial disturbances, pandemics, epidemics, health emergencies, virus, disease, plague, quarantine, travel restrictions, acts of governmental agencies or authorities (whether or not such acts are made in response to other Force Majeure Events), or any other circumstances, events or contingencies not within the reasonable control of the party affected, whether or not of a similar kind or nature to any of the foregoing (a "Force

Majeure Event"). The party seeking application of this provision shall notify the other party in writing promptly upon learning of the impact of the Force Majeure Event upon the notifying party's performance of its obligations under this Agreement.

15. DISPUTE AVOIDANCE AND RESOLUTION

15.1. The parties will attempt in good faith to resolve through negotiation any dispute, claim, counterclaim, or controversy arising out of or relating to this Agreement (hereafter collectively referred to as "Dispute"). If the Dispute is not resolved by these negotiations, the parties agree to submit any such unresolved Dispute to mediation. Either party may commence mediation by providing the other party a written request for mediation, setting forth the subject of the Dispute and the relief requested. The parties will cooperate with one another in selecting a mediator, and in scheduling the mediation proceedings. The parties will share equally in the costs of the mediator. Neither party may commence a civil action with respect to the matters submitted to mediation until after the completion of the initial mediation session, or 45 days after the date of filing the written request for mediation, whichever occurs first. Mediation may continue after the commencement of a civil action, if the parties so desire. The provisions of this paragraph may be enforced by any court of competent jurisdiction.

16. MISCELLANEOUS

16.1. Notices. Each Party shall deliver all notices, requests, consents, claims, demands, waivers, and other communications under this Agreement (each, a "Notice") in writing and addressed to the other Party at the addresses set forth on the first page of this Agreement (or to such other address that the receiving Party may designate from time to time in accordance with this section). Each Party shall deliver all Notices by personal delivery, nationally recognized overnight courier (with all fees prepaid), facsimile [or email] (with confirmation of transmission), or certified or registered mail (in each case, return receipt requested, postage prepaid). Except as otherwise provided in this Agreement, a Notice is effective only (a) upon receipt by the receiving party and (b) if the party giving the Notice has complied with the requirements of this Section.

16.2. Governing Law. Irrespective of the place of performance, this Agreement and any disputes arising out of, or relating to, this Agreement shall be governed by the laws of the State of Florida (without regard to the conflict of law rules) and federal laws of the United States. This Agreement excludes the application of the 1980 United Nations Convention on Contracts for the International Sale of Goods.

16.3. Assignment. Customer shall not assign or otherwise transfer any of its rights or delegate or otherwise transfer any of its obligations or performance under this Agreement, in each case whether voluntarily, involuntarily, by operation of law, or otherwise, without Conquest Cyber's prior written consent, which consent shall not be unreasonably withheld, conditioned, or delayed. Any purported assignment, delegation, or transfer in violation of this Section 16.3 is void. This Agreement is binding upon and inures to the benefit of the parties hereto and their respective successors and permitted assigns.

16.4. Joint Preparation. The parties expressly agree that this Agreement shall be construed neither against nor in favor of either party but shall be construed in a neutral manner.

16.5. Effect of Waiver. The failure of either party to insist on strict compliance with any of the terms, covenants, or conditions of this Agreement by the other party shall not be deemed a waiver of that term, covenant, or condition, nor shall any waiver or relinquishment of any right or power at any time or times be deemed a waiver or relinquishment of that right or power for all or any other times.

16.6. Severability. If any provision in this Agreement is held by a court of competent jurisdiction to be invalid, void, or unenforceable, the remaining provisions shall nevertheless continue in full force without being impaired or invalidated in any way.

16.7. Headings. The headings in this Agreement are for reference only and do not affect the interpretation of this Agreement.

Entire Agreement. This Agreement contains the entire Agreement of the parties hereto with respect to the subject matter hereof; all prior agreements, understandings, statements, promises and any and all existing contracts previously executed by the parties are hereby void.

Appendix B: Service Level Agreement

This Service Level Agreement ("SLA") forms part of the Order Form between Conquest Cyber and Customer, under which Conquest Cyber delivers certain products and services for Customer. It sets forth the parties' objectives and the performance levels Conquest Cyber must meet for all included services. This SLA is effective beginning on the Term Start Date as set forth in the Order Form and will remain in effect until the termination of the Order Form.

The parties intend to review this SLA on either party's reasonable request. Any revisions to the service levels must be authorized by both parties in accordance with the change order processes set forth in the Order Form Terms and Conditions.

DEFINITIONS

"System Availability" means Conquest Cyber systems and software are fully operational, and Customer can access the ARMED ATK SECOPS Module, and are able to receive, process, store, and respond to Customer requests. Scheduled maintenance windows are excluded from availability metrics provided Conquest provides written communication in advance of the maintenance event.

"Key Performance Indicator (KPI)" - A service level measurement that is not subject to service credits, but that is important to the Customer's business. Upon not less than 30 days' reasonable notice, the Customer may request that a KPI be converted to a Service Level, in which case the parties will negotiate in good faith a Service Credit applicable to such measurement. The parties will amend this SLA (Service Level Agreement) to reflect any such change.

"Investigation and Triage" - Conquest Cyber is responsible for incident detection, analysis, investigation, and escalation. It is the primary responsibly of Conquest Cyber to ensure that security events and incidents are detected and escalated in a timely manner.

"Mean Time to Detect (MTTD)" - Measures timeframe (minutes) from initial event detection by the Security Information Event Management (SIEM) to the time when the case is opened within the Conquest ARMED ATK platform. This is an automated system measurement to determine the health in receiving logs for analyst response. Spikes in this metric indicate issues with log collection, network latency issues between customer network and Conquest, system outages, or integration failures.

"Mean Time to Triage (MTTT)" - Measures timeframe (minutes) from initial event detection by the Security Information Event Management (SIEM) and the assignment to a Conquest Security Operations Center (SOC) Analyst for triage and initial investigation within the ARMED ATK platform. The SLA timeframe in minutes is automatically calculated by the Conquest XSOAR platform and annotated in the case log.

"Mean Time to Resolution (MTTR)" - Measures from initial event detection by the Security Information Event Management (SIEM) until either the closure of a case, escalation to the customer, or escalation to a Conquest tier 3 analyst for more in-depth investigation, including the documented root cause analysis or up-to-date investigation and case notes. Please Note that the overall resolution of a case is a shared SLA between the SOC and the customer investigation of cases does not stop with escalation to the customer, but case closure may require customer input and collaboration that is affected by customer shift schedule and resource availability.

"Service Credit" means a percentage of Service Fees to be credited to Customer if Conquest Cyber fails to meet a Service Level, as set forth in this SLA.

"Service Level" means a performance standard Conquest Cyber must meet in providing the Services, as set forth in this SLA.

1. Terms and Conditions
   1.1. No Service Credit will exceed an aggregate of two percent (2%) of Customer's monthly fees for the Service feature in question for the then-current billing month. Any Service Credit payable to Customer under this Agreement will be issued to Customer in the calendar month following the Service Period in which the Service Level Failure occurred. This Section 2 sets forth Conquest Cyber's sole obligation and Customer's sole remedy for any Service Level Failure.

   1.2. The deployment of Conquest Cyber's managed security services in the Customer's network does not guarantee that intrusions, compromises, or any other unauthorized activity will not occur on a customer's network.

   1.3. Conquest may schedule maintenance outages for Conquest owned equipment/servers, which are being utilized to perform the services, with 24 hours' notice to designated Customer contacts. The Service Levels shall not apply during scheduled maintenance outages and, therefore, are not eligible for any Service Level credit.

1.4. The Service Levels shall not apply in the event of any Customer-caused service outage that prohibits or otherwise limits Conquest from providing the Service or delivering the Service Levels or managed service descriptions, including, but not limited to, Customer's misconduct, negligence, inaccurate or incomplete information, modifications made to the Services, or any unauthorized modifications made to any managed hardware or software devices by Customer, its employees, agents, or third parties acting on behalf of Customer.

1.5. Conquest Cyber will be responsible for incident analysis, case enrichment, and investigation to determine if alerts or security events warrant incident classification. If an event is classified as an incident by Conquest Cyber, then Conquest Cyber will be responsible for tracking the incident with the customer through final resolution. The Conquest Cyber team will perform incident triage to include determining scope, urgency, and potential impact, and will identify specific vulnerabilities and make recommendations to allow for remediation.

1.6. Conquest Cyber will be the focal point for organizational security issues. Conquest Cyber will be the collection point for additional group inputs for the classification of security incidents. The potential exists for other entities to notify Conquest Cyber of events. In these rare cases, Conquest Cyber will ensure outside sources of information are incorporated into established Conquest Cyber workflow procedures. As events are pulled into the Conquest Cyber Workflow, it is Conquest Cyber's responsibility to create and classify incidents. Conquest Cyber is responsible for incident escalation and response, only Conquest Cyber has the authority to classify events or alerts as incidents to ensure due diligence of event investigation and accountability in reporting

2. Assumptions:

Conquest's performance of the Services under this SLA is subject to the following assumptions, constraints, and dependencies:

2.1. The Service Levels shall not apply to the extent Customer does not fulfill and comply with its obligations and interdependencies set forth within this SLA.

2.2. The obligations of Conquest to comply with the Service Levels with respect to any incident response or help desk requests are also interdependent on Conquest's ability to connect directly to Customer's devices on Customer's network through an authenticated server in the Conquest Cyber Security Operations Center (SOC).

2.3. Information provided by Customer to Conquest as required for the Services will be accurate and timely.

2.4. Conquest's procedures and delivery of Services may be affected by changes in relevant Customer internal policies.

2.5. Any Service Credit payable to Customer under this Agreement will be issued to Customer in the calendar month following the Service Period in which the Service Level Failure occurred. This Section 2.5 sets forth Conquest Cyber's sole obligation and Customer's sole remedy for any Service Level Failure.

3. INCIDENT RESPONSE MATRIX

Service Level Agreements (SLA) are assessed for events based on two factors: event severity and device criticality. The event severity is determined by the Security Information Event Management (SIEM), as defined within deployed analytical detection rules. Device criticality is assigned through the association of an organization's hardware assets to one or more critical subsystems. The assignment of hardware assets to critical subsystems is performed within the ARMED ATK platform's "SHIELD" module. An organization's critical subsystems are defined within the ARMED ATK "Risk" module through the creation of overall IT Risk Management strategy.

All Service Level Agreement (SLA) metrics are aggregated as a monthly running average across all cases. At the end of each month SLA metrics are assessed over the period of the current month.

EVENT CLASSIFICATION	Event Priority	Conditions	Mean Time to Triage Times (MTTT)	Mean Time to Resolution MTTR or Escalation Time	Notification Method
Event Score > 9	1	The event is identified as a MEDIUM, HIGH, or CRITICAL severity event by the SIEM and the associated hardware device is identified by the organization as a "Critical" asset.	Avg < 1 hour	Avg < 6 hours	Portal, Email. Phone Call for any ***event severity*** of critical.
Event Score 7-9	2	The event is identified as a LOW, MEDIUM, HIGH, or CRITICAL severity event by the SIEM and the associated hardware device is identified by the organization as a "Medium" or "High" criticality asset.	Avg < 10 hours	Avg < 14 hours	Portal, Email
Event Score < 7	3	The event is identified as a LOW, MEDIUM, HIGH, or CRITICAL severity event by the SIEM and associated hardware device is identified by the organization as a "Low" criticality asset, or no device criticality is associated with the device.	Avg < 48 hours	Avg < 72 hours	Portal, Email

Security Operations Center (SOC) SLA metrics by Event Score. *Note: For all event scores, Conquest Security Operations Center (SOC) will initiate a phone call if an analyst investigation indicates high probability of compromise regardless of event severity for critical devices.*

4. Health Monitoring SLAs

Name	Description	Response Time	Notification Method
ARMED ATK Portal "SecOps" Module Availability and Notification Systems	Conquest provides access and the availability for customers to login successfully and view security case details within the ARMED SecOps Module. System availability shall be measured by the number of minutes in the month minus the number of minutes the SECOPS Module is unavailable during the month (adjusted for communicated downtime) divided by the total number of minutes in the month x 100. Scheduled downtime is announced via email, providing the start and end date and time for the window.	Overall Uptime 99.5% and communication within 2 hours	Email

ARMED ATK Portal Availability SLA Metrics. Note: These metrics exclude pre-scheduled and communicated maintenance events during which alternative communication and visibility into case status can be established

5. Service Level Credits

SLA	Definition	Credit
Incident Response Matrix	Customer will receive an electronic or a phone call notification of a security incident (in accordance with Customer's defined incident response procedures) according to the priority assigned to the event and the security monitoring SLA schedule given the event is determined to be an incident. This is measured by the difference between the time stamp of the incident ticket created by the Conquest Cyber SOC personnel or technology and the time stamp of the correspondence documenting the initial escalation. Security incidents generated from long-term correlation logic and retroactive analyses based on newly identified threat indicators are not subject to this SLA. Events deemed "informational" severity will not be escalated but will be available for reporting through the portal.	1% of the total monthly fee
ARMED ATK Portal "SecOps" Module Availability and Notification Systems	Conquest provides access and the ability for customer to login successfully and view security case details within the ARMED SecOps Module. System availability shall be measured by the number of minutes in the month minus the number of minutes the SECOPS Module is unavailable during the month to accept log feeds from the customer and process such data (adjusted for any scheduled downtime) divided by the total number of minutes in the month x 100.	1% of the total monthly fee