910 Calle Negocio
2nd Floor
San Clemente, California
www.san-clemente.org

AGENDA REPORT

CITY OF SAN CLEMENTE

City Council Meeting

Meeting Date: 6/6/2023 Agenda Item: 7H

Department: Information Technology
Prepared By Brian Brower, IT Manager

Subject:
CONSIDERATION OF FIRST AMENDMENT TO PROFESSIONAL SERVICES AGREEMENT FOR MANAGED SECURITY SERVICES WITH SAVANT SOLUTIONS, INC

Summary:
For the last three years, the City has used professional managed security services under an agreement (Attachment 1) with Savant Solutions, Inc. (Savant) to ensure the City's network and cyber defense mechanisms are actively monitored for attacks or malicious activity, and critical IT assets are protected from such activities. That agreement expires July 1, 2023. Before the City Council is the approval of a First Amendment to the Professional Services Agreement with Savant in an amount not to exceed $118,713, which includes $57,909 in year one and $60,804 in year two for the ongoing subscription, maintenance and support of the Arctic Wolf Networks Managed Detection and Response and Managed Risk security solutions.

Background:
On April 21, 2020, the City awarded contract C20-21 (Attachment 1) to Savant for the implementation of the Arctic Wolf Networks Managed Detection and Response and Managed Risk Services, which included three years of Subscription, Maintenance and Support fees. For the past three years, the City has contracted cybersecurity services from this Managed Security Services Provider (MSSP) to assist the IT Division in securing the City's network and other IT resources. The total cost of the original agreement was $181,945 over the three year term, including equipment, implementation and training, subscription, maintenance and support fees, and a one-time penetration test/vulnerability assessment.

The MSSP delivers several critical services including network monitoring, log aggregation and analysis, incident and event management, intrusion detection and prevention, and vulnerability scanning. The service includes 24x7x365 real-time monitoring of perimeter firewalls, network equipment, critical servers, and email system, providing event correlation and log analysis along with incident detection, response, and risk mitigation capabilities. These services ensure the City's network and cyber defense mechanisms are actively monitored for attacks or malicious activity, and critical IT assets are protected from such activities.

The solution incorporates a complete, managed Security Information and Event Management (SIEM) service, ongoing operation and support, and all related equipment and software. The solution aggregates and analyzes security information by ingesting both real-time data and stored logs for the purpose of incident identification and response, and includes continuous monitoring of City network security equipment and real-time analysis and alerts, focusing on actionable events for customer

notification and remediation.

The system gathers event data from monitored devices, forwards such data to a secure operations center, analyzes the data, and report findings to the appropriate City personnel via phone and email. The service also includes an integrated electronic dashboard with real-time monitoring, analysis and reporting functions.

Major elements of the current service include the following:

- AWN Managed Detection and Response (MDR) cloud-based managed SIEM system to continuously monitor the City's computing environment and ensure proactive detection and response to threats and attacks. The service collects, analyzes and correlates data from servers, devices and network traffic. This service includes the ability to invoke containment to quarantine a compromised device.

- Security Engineer to act as an extension of the City's IT team and secondary analyst to become familiar with the City's network and environment, provide 24x7x365 support, and ensure a single point of contact to monitor, prioritize, and help remediate security issues.

- AWN MDR Office 365 service for continuous monitoring and threat detection on the City's cloud-based email system.

- AWN Sensor to provide real-time monitoring of on-premise network data flow to detect advanced threats such as anomalous network behavior, botnets, exploits and malware.

- AWN Managed Risk service to continuously scan all networks and endpoints and quantify risks and vulnerabilities, and provide a prioritized remediation plan in order to improve the City's cyber-risk posture. Managed Risk also includes Dark Web scan to monitor data leaks for City information or credentials.

- Service Level Agreement (SLA) providing 24x7x365 availability to security engineers with a response time of 60 minutes for routine calls, 30 minutes for Emergency incidents detected by Arctic Wolf Networks, and five minutes if reported as an Emergency by the City.

As proposed, the First Amendment to the Professional Services Agreement with Savant would provide a two year extension of the current subscription services. A cost breakdown of the First Amendment is provided below:

Year 1: Ongoing Subscription, Maintenance and Support	$57,909
Year 2: Ongoing Subscription, Maintenance and Support	$60.804
Total Two Year Cost:	$118,713

Funding for a managed Security Information and Event Management solution is included in the FY 2023-24 Proposed Budget.

Council Options:

- Adopt Resolution No. 23-36, authorizing the City Manager to execute the First Amendment to the Professional Services Agreement with Savant Solutions, Inc.
- Adopt Resolution No. 23-36, with modifications.
- Continue the Item and direct staff to provide additional information.
- Do not Adopt Resolution No. 23-36 and allow the Professional Services Agreement with Savant to expire.

Fiscal Impact:

Yes. The total amount of the First Amendment is not to exceed $118,713 over a two year period, including subscription, maintenance and support fees. The year one amount of $57,909 is currently budgeted in the Information Technology Fund in account 063-241-43456.

Environmental Review/Analysis:

This is not a “project” under the California Environmental Quality Act.

Recommended Actions:

Staff Recommendation

Adopt Resolution No. 23-36, authorizing the City Manager to execute the First Amendment to Professional Services Agreement with Savant Solutions, Inc. for a total contract amount not to exceed $300,658, which includes an additional $118,713 for the two year extension of the Arctic Wolf Networks Managed Detection and Response and Managed Risk Services through July 1, 2025.

Attachment:

1. Professional Services Agreement with Savant Solutions, Inc. dated April 21, 2020
2. Proposal for Two Year Extension of Managed Risk / Managed Detection and Response Service by Arctic Wolf Networks, Inc. and Savant Solutions, Inc.
3. Resolution No. 23-36
4. DRAFT First Amendment to Professional Services Agreement with Savant Solutions, Inc.

Notification:

None

PROFESSIONAL SERVICES AGREEMENT FOR MANAGED SECURITY SERVICES

THIS PROFESSIONAL SERVICES AGREEMENT (the "Agreement") is made and entered into this 21st day of April, 2020 (the "Effective Date"), by and between the City of San Clemente, a municipal corporation, hereinafter referred to as the "CITY", and Savant Solutions of 1007 7th St., 5th Floor, Sacramento, CA 95814 hereinafter referred to as the "CONTRACTOR".

RECITALS:

A. CITY requires professional **Managed Security** services to be performed at or in connection with **Security Information and Event Management (SIEM) and Vulnerability Assessment**.

B. CONTRACTOR has represented to CITY that CONTRACTOR is qualified to perform said services and has submitted a proposal to CITY for same.

C. CITY desires to have CONTRACTOR perform said services on the terms and conditions set forth herein.

COVENANTS:

Based on the foregoing Recitals and for good and valuable consideration, the receipt and sufficiency of which is acknowledged by both parties, CITY and CONTRACTOR agree as follows:

ARTICLE 1
RESPONSIBILITIES OF CONTRACTOR

1.1 Term.

The term of this Agreement shall commence on the Effective Date, and shall continue and remain in effect, until **July 1, 2023**, unless terminated earlier pursuant to the terms hereof. Notwithstanding the forgoing, the City Manager or his or her designee shall have the authority on behalf of the City to administratively approve extensions to the term hereof not to exceed a cumulative total of one hundred eighty (180) days.

1.2 Scope of Services.

CONTRACTOR shall perform any and all work necessary for the completion of the tasks and services set forth in the "Scope of Services" attached hereto and incorporated herein as Exhibit "A" in a manner satisfactory to CITY. By execution of this Agreement, CONTRACTOR warrants that (i) it has thoroughly investigated and considered the work

to be performed; (ii) it has carefully examined the location or locations at or with respect to which the work is to be performed, as applicable; and (iii) it fully understands the difficulties and restrictions attending the performance of the work provided for under this Agreement. CONTRACTOR acknowledges that certain refinements to the Scope of Services may, on occasion, be necessary to achieve CITY's goals hereunder, and CONTRACTOR shall cooperate with and assist the CITY to identify and make such refinements prior to undertaking any tasks or services that may require refinement.

1.3 Schedule of Performance.

Prior to the City's execution of this Agreement, and as a condition to the effectiveness hereof, CONTRACTOR shall furnish to CITY proof of insurance coverage as required under Article 5, Insurance. Upon CITY's release to CONTRACTOR of a fully executed copy hereof and issuance of a written Notice to Proceed, CONTRACTOR shall promptly commence performance of the work. Until such time, CONTRACTOR is not authorized to perform and will not be paid for performing any work under this Agreement. CONTRACTOR shall exercise reasonable diligence to have the services as set forth in Exhibit "A" completed and submitted to CITY for final approval as soon as reasonably practicable and in accordance with the schedule of performance attached hereto and incorporated herein as Exhibit "B", provided that CONTRACTOR shall be entitled to an extension of time for any delays caused by events or occurrences beyond CONTRACTOR's reasonable control.

1.4 Identity of Persons Performing Work.

CONTRACTOR represents that it employs or will employ at its own expense all personnel required for the satisfactory performance of any and all tasks and services required hereunder. CONTRACTOR shall not replace any of the principal members of the Project team, including any of the persons listed in Exhibit "A" (if CONTRACTOR'S personnel is listed on Exhibit "A"), or any successors to any of such persons, without CITY's prior written approval.

CONTRACTOR represents that the tasks and services required hereunder will be performed by CONTRACTOR or under its direct supervision, and that all personnel engaged in such work shall be fully qualified and shall be authorized and permitted under applicable State and local law to perform such tasks and services. In carrying out such tasks and services, CONTRACTOR shall not employ any undocumented aliens (i.e., persons who are not citizens or nationals of the United States).

This Agreement contemplates the personal services of CONTRACTOR and CONTRACTOR's employees, and it is recognized by the parties hereto that a substantial inducement to CITY for entering into this Agreement was, and is, the professional reputation and competence of CONTRACTOR and CONTRACTOR's employees. Neither this Agreement nor any interest therein may be assigned by CONTRACTOR, except upon written consent of CITY.

Furthermore, CONTRACTOR shall not subcontract any portion of the performance contemplated and provided for herein without the prior written approval of CITY, except for those subcontractors named in the proposal for the project. Nothing herein contained is intended to or shall be construed as preventing CONTRACTOR from employing or hiring as many employees as CONTRACTOR may deem necessary for the proper and efficient execution of this Agreement.

1.5 Cooperation and Coordination of Work With CITY.

CONTRACTOR shall work closely with CITY's designated representative, either individual or committee, who shall have the principal responsibility for liaison and who shall, on a continuous basis, review and approve CONTRACTOR's work. CONTRACTOR shall ensure that CITY has reviewed and approved all required work as the project progresses.

1.6 Compliance With Laws.

CONTRACTOR shall comply with all applicable Federal, State and local laws, ordinances and regulations, including without limitation all applicable fair labor standards. CONTRACTOR shall not discriminate against any employee or applicant for employment or any approved subcontractor, agent, supplier or other firm or person providing services to CONTRACTOR in connection with this Agreement on the basis of race, color, creed, ancestry, national origin, religion, sex, sexual orientation, marital status, or mental or physical disability. CONTRACTOR shall take affirmative action to ensure that applicants are employed, and that employees are treated during their employment, without regard to their race, color, creed, ancestry, national origin, religion, sex, sexual orientation, marital status, and mental or physical disability. Such actions shall include, but not be limited to the following: employment, upgrading, demotion or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship.

Prior to execution of this Agreement, CONTRACTOR shall furnish to CITY proof that CONTRACTOR and all of its subcontractors have a current, valid business license issued by CITY.

1.7 Standard of Performance.

CONTRACTOR acknowledges and understands that the services and work contracted for under this Agreement require specialized skills and abilities and that, consistent with this understanding, CONTRACTOR's services and work shall be held to a standard of quality and workmanship prevalent in the industry for such service and work. CONTRACTOR represents to CITY that CONTRACTOR holds the necessary skills and abilities to satisfy the standard of work as set forth in this Agreement. CONTRACTOR shall perform the work and services under this Agreement in accordance with such standard of work and in accordance with the accepted standards of the professional disciplines involved in the project. All work shall be completed to the reasonable satisfaction of CITY. If CITY

reasonably determines that the work is not satisfactory, CITY shall have the right to: (i) meet with CONTRACTOR to review CONTRACTOR's work and resolve matters of concern; and/or (ii) require CONTRACTOR to repeat unsatisfactory work at no additional charge until it is satisfactory.

1.8 Contractor Ethics.

CONTRACTOR represents and warrants that it has not provided or promised to provide any gift or other consideration, directly or indirectly, to any officer, employee, or agent of CITY to obtain CITY's approval of this Agreement. CONTRACTOR shall not, at any time, have any financial interest in this Agreement or the project that is the subject of this Agreement other than the compensation to be paid to CONTRACTOR pursuant to Article 3, Compensation. In the event the work and/or services to be performed hereunder relate to a project and/or application under consideration by or on file with the City, (i) CONTRACTOR shall not possess or maintain any business relationship with the applicant or any other person or entity which CONTRACTOR knows to have a personal stake in said project and/or application, (ii) other than performing its work and/or services to CITY in accordance with this Agreement CONTRACTOR shall not advocate either for or against said project and/or application, and (iii) CONTRACTOR shall immediately notify CITY in the event CONTRACTOR determines that CONTRACTOR has or acquires any such business relationship with the applicant or other person or entity which has a personal stake in said project and/or application. The provisions in this Section 1.8 shall be applicable to all of CONTRACTOR's officers, directors, employees, and agents, and shall survive the termination of this Agreement.

1.9 Changes and Additions to Scope of Services.

CITY may make changes within the general scope of services provided for in this Agreement. CONTRACTOR shall agree to any such changes that are reasonable. CONTRACTOR shall make no change in or addition to the character or extent of the work required by this Agreement except as may be authorized in advance in writing by CITY. Such supplemental authorization shall set forth the specific changes of work to be performed and related extension of time and/or adjustment of fee to be paid to CONTRACTOR by CITY.

1.10 Hiring of Illegal Aliens Prohibited

CONTRACTOR shall not hire or employ any person to perform work within the City of San Clemente or allow any person to perform work required under this Agreement unless such person is a United States citizen or is properly documented and legally entitled to be employed within the United States.

1.11 Endorsement on PS&E/Other Data

CONTRACTOR shall sign all plans, specifications, estimates (PS&E) and engineering data furnished by CONTRACTOR, and where appropriate will indicate CONTRACTOR's authorized signature and professional registration number.

ARTICLE 2
RESPONSIBILITIES OF CITY

2.1 Provision of Information.

CITY shall provide full information regarding its requirements for the project, and it shall furnish, without charge to CONTRACTOR, any and all information, data, plans, maps and records which are available to CITY and are necessary for the provision by CONTRACTOR of the tasks and services set forth herein.

2.2 Cooperation With CONTRACTOR.

CITY shall cooperate with CONTRACTOR in carrying out the work and services required hereunder without undue delay. In this regard, CITY, including any representative thereof, shall examine plans and documents submitted by CONTRACTOR, shall consult with CONTRACTOR regarding any such plans and documents, and shall render any necessary decisions pertaining to such plans and documents as promptly as is practicable.

ARTICLE 3
PAYMENT

3.1 Payment Schedule: Maximum Payment Amount.

Prior to the tenth of the month, CONTRACTOR shall submit to CITY a monthly status report and invoices itemizing the services rendered during the previous month. Within fifteen (15) working days after receipt of an invoice from CONTRACTOR, CITY shall determine whether and to what extent CONTRACTOR has adequately performed the services for which payment is sought. If CITY determines that CONTRACTOR has not adequately performed such services, CITY shall inform CONTRACTOR of those acts which are necessary for satisfactory completion. Subject to the provisions of Section 5.2 below, which provide for the City to withhold payment in the event CONTRACTOR's insurance expires during the term of this Agreement, CITY shall cause payment to be made to CONTRACTOR within fifteen (15) working days from CITY's determination that CONTRACTOR has adequately performed those services for which CITY has been invoiced. In no case shall CITY pay in excess of each line item set forth in Exhibit "A" for any particular task unless approved and authorized by the CITY in writing (applicable only if Exhibit "A" breaks down the Scope of Services on a line item basis). The total compensation for the Scope of Services set forth in Exhibit "A" shall not exceed One Hundred and Eighty One Thousand, Nine Hundred and Forty Five Dollars ($181,945),

including all amounts payable to CONTRACTOR for its overhead, payroll, profit, and all costs of whatever nature, including without limitation all costs for subcontracts, materials, equipment, supplies, and costs arising from or due to termination of this Agreement (the "Total Compensation").

3.2 Changes in Work.

If CONTRACTOR estimates that any proposed change within the general scope of services set forth in Exhibit "A" causes an increase or decrease in the cost and/or the time required for performance of this Agreement, CONTRACTOR shall so notify CITY of that fact in advance of commencing performance of such work. Any such change, and the cost for such change, shall be agreed upon by CITY and CONTRACTOR, and reduced to a writing that, once signed by both CITY and CONTRACTOR, shall modify this Agreement accordingly. In determining the amount of any cost increase for such change, the value of the incomplete portions of the original tasks and services affected by the change shall be credited back to CITY.

3.3 Additional Work.

CITY may request CONTRACTOR to perform additional services not covered by the specific scope of services set forth in Exhibit "A", and CONTRACTOR shall perform such extra services and will be paid for such extra services when the extra services and the cost thereof are reduced to writing, signed by both CITY and CONTRACTOR, and made a part of this Agreement. CITY shall not be liable for payment of any extra services nor shall CONTRACTOR be obligated to perform any extra services except upon such written amendment. To the extent that the extra services render all or a portion of the original tasks and services unnecessary, the value of the unnecessary and incomplete portions of original tasks and services shall be credited back to CITY.

ARTICLE 4
INDEPENDENT CONTRACTOR

CONTRACTOR is an independent contractor and not an employee of the CITY. Neither the CITY nor any of its employees shall have any control over the conduct of the CONTRACTOR or any of CONTRACTOR's employees, except as herein set forth, and CONTRACTOR expressly warrants not to, at any time or in any manner, represent that CONTRACTOR, or any of CONTRACTOR's agents, servants or employees, are in any manner agents, servants or employees of the CITY, it being distinctly understood that CONTRACTOR is and shall at all times remain as to the CITY a wholly independent contractor and that CONTRACTOR's obligations to the CITY are solely such as are prescribed by this Agreement.

ARTICLE 5
INDEMNITY AND INSURANCE

5.1 Indemnification

FOLLOWING PARAGRAPH APPLICABLE TO AGREEMENTS WHERE CONTRACTOR IS A "LICENSED DESIGN PROFESSIONAL" AND IS PROVIDING DESIGN PROFESSIONAL SERVICES:

To the fullest extent permitted by law (including, without limitation, California Civil Code Sections 2782 and 2782.6), CONTRACTOR shall defend (with legal counsel reasonably acceptable to the CITY), indemnify, and hold free and harmless CITY and CITY's agents, officers, and employees, and the San Clemente Redevelopment Agency and its agents, officers, and employees (collectively, the "Indemnitees") from and against any and all claims, loss, cost, damage, injury (including, without limitation, injury to or death of CONTRACTOR or any officers, agents, employees, representatives, or subcontractors of CONTRACTOR [collectively, the "CONTRACTOR ENTITIES"]), expense and liability of every kind, nature and description (including, without limitation, incidental and consequential damages, court costs, attorney's fees, litigation expenses and fees of expert Contractors or expert witnesses incurred in connection therewith and costs of investigation) that arise out of, pertain to, or relate to, directly or indirectly, in whole or in part, the negligence, recklessness, or willful misconduct of CONTRACTOR, any of the CONTRACTOR ENTITIES, anyone directly or indirectly employed by any of them, or anyone that they control (collectively, the "Liabilities"). Such obligation to defend, hold harmless and indemnify any Indemnitee shall not apply to the extent that such Liabilities are caused in part by the sole negligence, active negligence, or willful misconduct of such Indemnitee.

FOLLOWING PARAGRAPH APPLICABLE TO AGREEMENTS WHERE CONTRACTOR IS NOT A "LICENSED DESIGN PROFESSIONAL":

CONTRACTOR shall defend (with legal counsel reasonably acceptable to the CITY), indemnify, and hold free and harmless CITY and CITY's agents, officers, and employees, and the San Clemente Redevelopment Agency and its agents, officers, and employees from and against any and all claims, loss, cost, damage, injury (including, without limitation, injury to or death of an employee of CONTRACTOR or CONTRACTOR's officers, agents, employees, representatives, or subcontractors [collectively, the "CONTRACTOR ENTITIES"]), expense and liability of every kind, nature and description (including, without limitation, incidental and consequential damages, court costs, attorney's fees, litigation expenses and fees of expert Contractors or expert witnesses incurred in connection therewith and costs of investigation) that arise out of, pertain to, or relate to, directly or indirectly, in whole or in part, the actions or failure to act of CONTRACTOR, any of the CONTRACTOR ENTITIES, anyone directly or indirectly employed by any of them, or anyone that they control, under this Agreement.

For purposes of this Agreement, a "Licensed Design Professional" shall be limited to licensed architects, registered professional engineers, licensed professional land surveyors and landscape architects, all as defined under current law, and as may be amended from time to time by California Civil Code § 2782.8.

5.2 Insurance.

Prior to the City's execution of this Agreement, and as a condition to the effectiveness hereof, CONTRACTOR shall submit certificates and endorsements to CITY indicating compliance with the following minimum insurance requirements, and CONTRACTOR shall maintain such insurance in effect during the entire term of this Agreement:

A. Workers' Compensation insurance to cover CONTRACTOR's employees as required by the California Labor Code with employer's liability limits not less than One Million Dollars ($1,000,000) per accident or disease. Before execution of this Agreement by CITY, CONTRACTOR shall file with CITY the attached signed Worker's Compensation Insurance Certification. CONTRACTOR shall require all subcontractors similarly to provide such compensation insurance for the respective employees.

None of the CITY, the San Clemente Redevelopment Agency, or any of their respective officers, employees, and agents will be responsible for any claims in law or equity occasioned by failure of CONTRACTOR to comply with this paragraph.

B. Commercial General Liability, personal injury and property damage liability, contractual liability, independent contractor's liability, and automobile liability insurance, with minimum combined liability limits of One Million Dollars ($1,000,000) per occurrence for all covered losses, and Two Million Dollars ($2,000,000) in the aggregate. Any deductible or self-insured retention in excess of Five Thousand Dollars ($5,000) shall be declared to the City and requires the prior approval of the City's Risk Manager. Each such policy of insurance shall:

(1) be issued by companies that hold a current policy holder's alphabetic and financial size category rating of not less than A-VII, according to the current Best's Key Rating Guide or a company of equal financial stability that is approved by CITY's Risk Manager for all coverages except surety.

(2) name and list as additional insureds CITY, CITY's officers, employees, and agents and, if the CITY's Risk Manager so requires, the City of San Clemente Redevelopment Agency and its officers, employees, and agents. An endorsement shall accompany the insurance certificate naming such additional insureds.

(3) specify it acts as primary insurance and that no insurance held or owned by CITY (or, if applicable, the San Clemente Redevelopment Agency) shall be called upon to cover a loss under said policy;

(4) contain a clause substantially in the following words: "it is hereby understood and agreed that this policy may not be canceled or materially changed except upon thirty (30) days prior written notice to CITY of such cancellation or material change as evidenced by a return receipt for a registered letter;"

(5) cover the operations of CONTRACTOR pursuant to the terms of this Agreement; and

(6) be written on an occurrence and not a claims made basis.

C. Professional Liability or Errors and Omissions insurance specifically designed to protect against acts, errors or omissions of the CONTRACTOR and "covered professional services" as designated in the policy must specifically include work performed under this Agreement. The policy limit shall be not less than One Million Dollars ($1,000,000) per claim and One Million Dollars ($1,000,000) in the aggregate. The policy must "pay on behalf of" the insured and must include a provision establishing the insurer's duty to defend.

If this box is checked and CITY has initialed below, the requirement for Professional Liability or Errors and Omissions insurance set forth in paragraph C above is hereby waived.

CITY's Initials: _____

Notwithstanding anything herein to the contrary, in the event any of CONTRACTOR's insurance as required pursuant to this Section 5.2 expires during the term of this Agreement, CITY shall withhold any payment due to CONTRACTOR hereunder until such time as CONTRACTOR obtains replacement insurance that meets all of the applicable requirements hereunder and submits certificates and endorsements evidencing such insurance to CITY.

CONTRACTOR shall require all of its subcontractors to procure and maintain during the course of their subcontract work with CONTRACTOR insurance that complies with the foregoing minimum insurance requirements. CONTRACTOR shall obtain from such subcontractors and retain in its files certificates evidencing such compliance.

ARTICLE 6
TERMINATION

This Agreement may be terminated by CITY for any reason, with or without cause, upon written notice to CONTRACTOR. In such event, CONTRACTOR shall be compensated for all services performed and costs incurred up to the date of notification for which CONTRACTOR has not been previously compensated, plus termination expenses reasonably incurred and properly accounted for (but in no event to exceed the amount which, when combined with other amounts paid, exceeds the amount for any uncompleted task set forth in Exhibit "A", as applicable). Upon receipt of notice of termination from CITY, CONTRACTOR shall immediately stop its services, unless otherwise directed, and deliver to CITY all data, drawings, reports, estimates, summaries and such other information and materials as may have been accumulated by CONTRACTOR in the performance of this Agreement, whether completed or in process.

ARTICLE 7
MISCELLANEOUS

7.1 Ownership of Documents.

All reports, software programs, as well as original data collected, original reproducible drawings, plans, studies, memoranda, computation sheets and other documents assembled or prepared by CONTRACTOR or furnished to CONTRACTOR in connection with this Agreement shall be the property of CITY and delivered to CITY at completion of the project or termination of this Agreement, whichever occurs first. Copies of said documents may be retained by CONTRACTOR, but shall not be made available by CONTRACTOR to any individual or organization without the prior written approval of CITY.

Any use of completed documents for projects other than that covered by this Agreement and/or any use of uncompleted documents without specific written authorization from CONTRACTOR will be at CITY's sole risk and without liability or legal exposure to CONTRACTOR.

7.2 Notices.

Any notices to be given under this Agreement shall be given by enclosing the same in a sealed envelope, postage prepaid, and depositing the same in the United States mail, addressed to CONTRACTOR at 1007 7th St., 5th Floor, Sacramento, CA 95814, and to the City of San Clemente, 910 Calle Negocio, San Clemente, California 92673, Attention: Brian Brower, IT Manager.

7.3 Covenant Against Contingent Fees.

CONTRACTOR warrants that it has not employed or retained any company or person to solicit or secure this Agreement and that it has not paid or agreed to pay any company or

person any fee or commission from the award or making of this Agreement. For breach or violation of this warranty, CITY shall have the right to annul this Agreement without liability or, in its discretion, to deduct from the Agreement price or consideration, or otherwise recover, the full amount of such fee or commission.

7.4 Liquidated Damages.

APPLICABLE ONLY IF THIS BOX HAS BEEN CHECKED AND BOTH PARTIES HAVE INITIALED BELOW.

If CITY seeks monetary damages for CONTRACTOR'S failure to complete all of the services required hereunder by the completion date set forth in Exhibit "B" (the "Completion Date"), CONTRACTOR shall be required to pay to CITY _____ Dollars ($_____) per day for each day beyond the Completion Date that any of such services remain uncompleted; provided, however, that nothing herein shall be deemed to limit CITY's remedy for CONTRACTOR's failure to complete all services required hereunder by the Completion Date to seeking monetary damages, and CITY shall be entitled to pursue any other equitable remedy permitted by law, including, without limitation, specific performance.

THE PARTIES HERETO AGREE THAT THE AMOUNT SET FORTH IN THIS SECTON 7.4 (THE "DAMAGE AMOUNT") CONSTITUTES A REASONABLE APPROXIMATION OF THE ACTUAL DAMAGES THAT CITY WOULD SUFFER DUE TO CONTRACTOR'S FAILURE TO COMPLETE ALL OF THE SERVICES REQUIRED HEREUNDER BY THE COMPLETION DATE, CONSIDERING ALL OF THE CIRCUMSTANCES EXISTING ON THE EFFECTIVE DATE OF THIS AGREEMENT, INCLUDING THE RELATIONSHIP OF THE DAMAGE AMOUNTS TO THE RANGE OF HARM TO CITY, THAT REASONABLY COULD BE ANTICIPATED AND THE ANTICIPATION THAT PROOF OF ACTUAL DAMAGES WOULD BE COSTLY OR INCONVENIENT. THE DAMAGE AMOUNT SET FORTH IN THIS SECTION 7.4 SHALL BE THE SOLE DAMAGES REMEDY FOR CONTRACTOR'S FAILURE TO COMPLETE ALL OF THE SERVICES REQUIRED HEREUNDER BY THE COMPLETION DATE, BUT NOTHING IN THIS SECTION 7.4 SHALL BE INTERPRETED TO LIMIT CITY'S REMEDY FOR CONTRACTOR'S FAILURE TO COMPLETE ALL OF THE SERVICES REQUIRED HEREUNDER BY THE COMPLETION DATE TO SUCH A DAMAGES REMEDY. IN PLACING ITS INITIALS AT THE PLACES PROVIDED HEREINBELOW, EACH PARTY SPECIFICALLY CONFIRMS THE ACCURACY OF THE STATEMENTS MADE ABOVE AND THE FACT THAT EACH PARTY HAS BEEN REPRESENTED BY COUNSEL OR HAS HAD THE OPPORTUNITY TO BE REPRESENTED BY COUNSEL TO EXPLAIN THE CONSEQUENCES OF THE LIQUIDATED DAMAGES PROVISION AT OR PRIOR TO THE TIME EACH EXECUTED THIS AGREEMENT.

CONTRACTOR'S INITIALS: _____ CITY'S INITIALS: _____

Notwithstanding any of the above, nothing herein is intended to preclude the CITY's recovery of its attorney's fees and costs incurred to enforce this Section 7.4, as provided in Section 7.10 below.

7.5 Interpretation and Enforcement of Agreement.

This Agreement shall be construed and interpreted both as to validity and performance of the parties in accordance with the laws of the State of California. Legal actions concerning any dispute, claim, or matter arising out of or in relation to this Agreement shall be instituted and maintained in the Superior Court of the County of Orange, State of California, or in any other appropriate court with jurisdiction in such county, and CONTRACTOR agrees to submit to the personal jurisdiction of such court.

7.6 Disputes.

In the event of any dispute arising under this Agreement, the injured party shall notify the defaulting party in writing of its contentions by submitting a claim therefor. The injured party shall continue performance of its obligations hereunder so long as the defaulting party immediately commences to cure such default and completes the cure of such default with reasonable diligence and in no event to exceed 30 days after service of the notice, or such longer period as may be permitted by the injured party; provided, that if the default results in an immediate danger to the health, safety, and general welfare, CITY may take such immediate action as CITY deems warranted.

7.7 Retention of Funds.

CITY may withhold from any monies payable to CONTRACTOR sufficient funds to compensate CITY for any losses, costs, liabilities or damages suffered by CITY due to default of CONTRACTOR in the performance of the services required by this Agreement.

7.8 Waiver.

No delay or omission in the exercise of any right or remedy by a nondefaulting party shall impair such right or remedy or be construed as a waiver. CITY's consent or waiver of one act or omission by CONTRACTOR shall not be deemed to constitute a consent or waiver of CITY's rights with respect to any subsequent act or omission by CONTRACTOR. Any waiver by either party of any default must be in writing.

7.9 Rights and Remedies are Cumulative.

Except as may be expressly set forth in this Agreement, the rights and remedies of the parties are cumulative and the exercise by either party of one or more of such rights or remedies or other rights or remedies as may be permitted by law or in equity shall not preclude the exercise by such party, at the same or different times, of any other rights or remedies to which such party may be entitled.

7.10 Attorneys' Fees.

In the event either party commences an action against the other party arising out of or in connection with this Agreement, the prevailing party in such action shall be entitled to recover its reasonable costs and expenses, including without limitation reasonable attorneys' fees and costs. Attorneys' fees shall include attorneys' fees on any appeal, and in addition, a party entitled to attorneys' fees shall be entitled to all other reasonable costs for investigating such action, including the taking of depositions and discovery, expert witness fees, and all other necessary costs incurred in the litigation, suit, or other action requiring attorney time. All such fees shall be enforceable whether or not such action is prosecuted to final judgment.

7.11 Integrated Agreement.

This Agreement contains all of the agreements of the parties and cannot be amended or modified except by written agreement. No prior oral or written understanding shall be of any force or effect with respect to those matters covered in this Agreement.

7.12 Authority.

The persons executing this Agreement on behalf of the parties hereto warrant that they are duly authorized to execute this Agreement on behalf of said parties.

[APPLICABLE TO INDIVIDUAL CONTRACTORS ONLY]

7.13 Compliance with California Unemployment Insurance Code Section 1088.8:
Prior to signing the Contract, CONTRACTOR shall provide to CITY a completed and signed Form W-9, Request for Taxpayer Identification Number and Certification. CONTRACTOR understands that pursuant to California Unemployment Insurance Code Section 1088.8, the CITY will report the information from Form W-9 to the State of California Unemployment Development Department, and that the information may be used for the purposes of establishing, modifying, or enforcing child support obligations, including collections, or reported to the Franchise Tax Board for tax enforcement purposes.

[End – Signature page follows]

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be duly executed on the respective dates set forth opposite their signatures.

CITY OF SAN CLEMENTE

By: Laura Ferguson

Its: Mayor Pro Tem

Dated: 5/16, 2020

ATTEST:

Deputy

CITY CLERK of the City of
San Clemente, California

APPROVED AS TO FORM:
BEST BEST & KRIEGER

By: _____
City Attorney

APPROVED AS TO AVAILABILITY
OF FUNDING

By: _____
Finance Authorization

Savant Solutions, Inc.

("CONTRACTOR")

Contractor's License Number_____

By: Caleb Kwong

Its: CEO

Dated: April 24, 2020

SAVANT SOLUTIONS

ARCTIC WOLF

Methodology

Solution Overview

Arctic Wolf Networks Managed Detection and Response service monitors your environment to ensure proactive detection and response to threats, intrusions, and attacks. The service collects, analyzes, and correlates Active Directory information, server/client logs, and network traffic. You receive timely and actionable security intelligence without the noise of false positives.

Managed Detection and Response Benefits

- A proprietary cloud-based SIEM & onsite IDS sensors for log aggregation and correlation
- Continuous monitoring, analysis, and correlations of events, logs, and user information
- A Concierge Security Engineer who understands your IT & business provides a personalized service
- Fully managed incident detection and response 24x7x365
- Improve the City of San Clemente's overall network security posture
- Risk mitigation against breaches through early incident detection and response
- Threat and vulnerability management – Concierge Security Team
- Security compliance monitoring and audit support
- Customizeable service and alert profiles for The city of San Clemente
- Predictable and simple pricing; our business model matches The City of San Clemente's goals
- Monthly or on-demand external vulnerability assessments (IVA, EVA, and Dark WEb included with optional Managed Risk service)
- Custom alert rules, response management, and reporting capabilities (compliance reports)

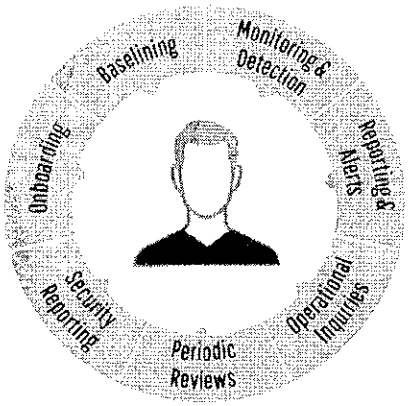
Concierge Security Engineer

Arctic Wolf Networks CyberSOC includes a Concierge Security Engineer ("CSE") who acts as an

SAVANT SOLUTIONS

ARCTIC WOLF

extension of your IT team. Your CSE configures and tunes the service to your technical and business requirements and monitors your security daily, making recommendations to help prioritize and resolve issues effectively. The CSE's goal is to eliminate false alerts, expose real threats, and adopt best practices for effective incident detection and response. By offloading the burden of log analysis and reporting, your CSE frees up your team's time to focus on your most strategic priorities for the organization.



- Dedicated Primary Contact
- Phone/Email/Text Support – 24x7x365
- Understands the City of San Clemente's Network & Business Goals
- Incident Detection & Response
- Proactive Threat Hunting
- Remote Forensic Analysis for Incidents
- Strategic Security Insights & Advice

The CSE team members are required to obtain the below certification depending on role within six months of hire/transition into role -

- Concierge Security Analyst - GSEC SANS 401. (GIAC Security Essentials Certification)
- Concierge Security Engineer - GCIH SANS 504. (GIAC Certified Incident Handler)

Our Security Services team hold various other industry certification obtained previous or while at Arctic Wolf networks, a non-exhaustive list is below –

- CISSP - Certified Information Systems Security Professional | (ISC2)
- CCSP - Certified Cloud Security Professional | (ISC2)
- HCISPP - HealthCare Information Security and Privacy Practitioner | (ISC2)
- Certified Ethical Hacker (CEH) - EC-Council
- GIAC Security Essentials Certification
- GCFE: GIAC Certified Forensic Examiner
- GCIH: GIAC Certified Incident Handler

SAVANT SOLUTIONS

ARCTIC WOLF

- GCIA: GIAC Certified Intrusion Analyst
- GICSP: Global Industrial Cyber Security Professional
- GXPN: GIAC Exploit Researcher and Advanced Penetration Tester
- Certified Penetration Tester (CPT) Boot Camp
- Certified Incident Handler (CIH)
- Offensive Security Certified Professional (OSCP) Certification

Service Details

Service Customization

- Build a customized escalation plan so that Arctic Wolf Networks has the correct information to get ahold of the City of San Clemente when a real incident occurs
- Continuously implement the learning loop into customized rules. (e.g., stop alerting about a server's outdated Java, but if it gets infected still alert, or alert the City of San Clemente every time an account is added to the Domain Admins Group)

Log aggregation

- Network IPFix logs, firewalls, servers, workstations, network devices, other security devices, Active Directory/DNS, etc. (*no log volume or source limits*)

Log retention

- Arctic Wolf can store logs from 90 days up to 10 years.

Detection & Response

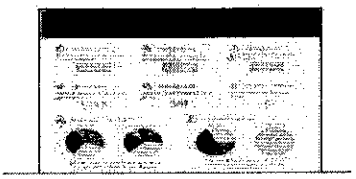
- Continuously review all data and perform forensics/triage on any anomalous data/incidents
- Report security incidents (after triage) in the manner that the City of San Clemente wants (e.g., email, phone, text, etc.)
- For each incident, prescribe a recommended remediation plan – Arctic Wolf CST provides this
- Forensic & malware analysis support when requested & as required to remediate or do root cause. (e.g., dynamic analysis on an executable via sandbox)

SAVANT SOLUTIONS

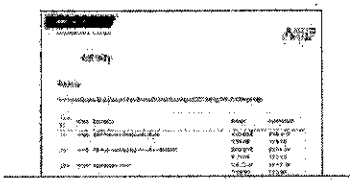
ARCTIC WOLF

Reports/Meetings

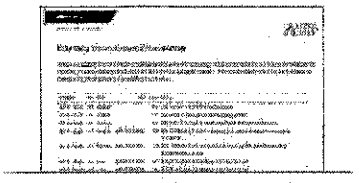
- Produce regular Monthly/Quarterly summaries
- On-demand internal and external vulnerability assessments through AWN CyberSOC/RootSecure
- Strategic Quarterly review meeting with prioritized security recommendation
- Monthly Security Report is included as an attachment to this RFP, but these other reports are available to review on request.



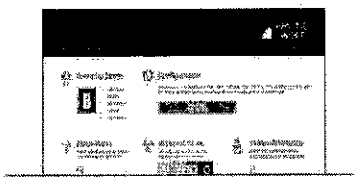
Security Review
Weekly/Monthly



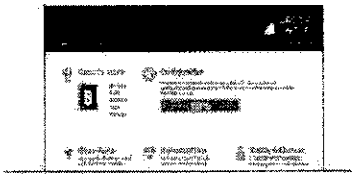
Open/Closed Incidents
Weekly



External Vulnerability
Monthly / On-Demand



Executive Summary
End of First Month



Monthly Assessment
Monthly

Quarterly Assessment
Quarterly (along with CSE/CSM meeting)

SAVANT SOLUTIONS

ARCTIC WOLF

Technology

The AWN CyberSOC service provides the capabilities of a world-class Security Operations Center (SOC), staffed by security experts and delivered as a service. The AWN CyberSOC service uses multiple tools and techniques to detect advanced threats including:

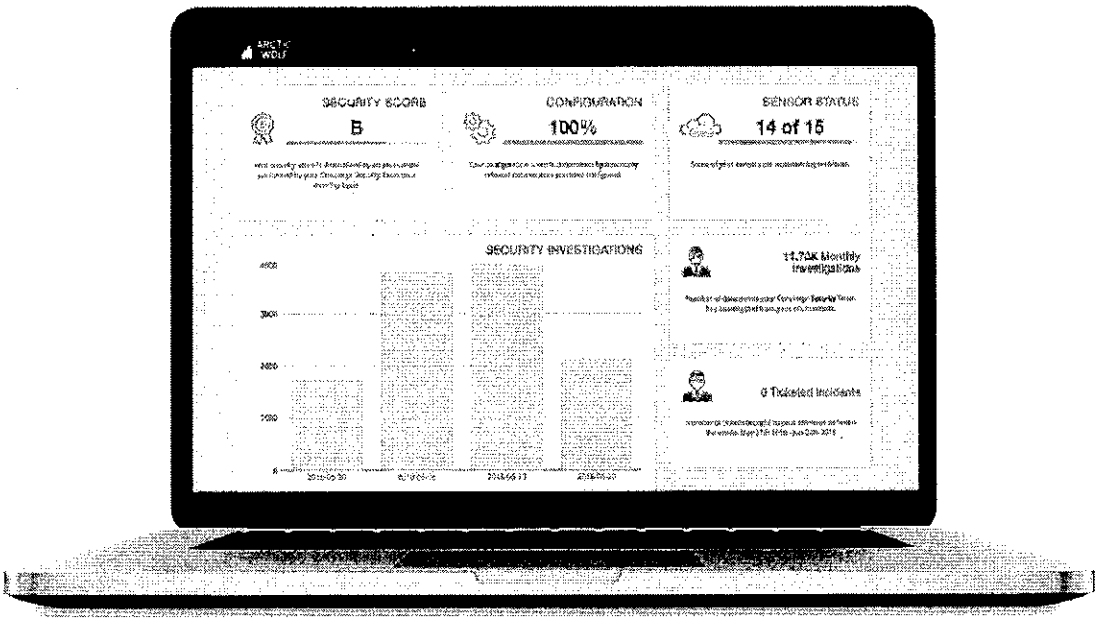
- Arctic Wolf Networks sensor: Deployed in your network, this sensor is an enterprise IDS that operates on flow data and uses a signature based approach to detect advanced threats. It uses a dataset comprised of over 40,000 rules covering over 45 categories including protocol specific attacks, network behaviors, botnets, vulnerabilities, exploits, malware command and control, SCADA network protocols, exploit kit activity and more. There are between 10 and 50 new rules created daily to detect emerging or newly discovered threats and your sensor's ruleset is updated with the latest information available every 24 hours. This sensor is also leveraged as a SYSLOG target and is used as the transport mechanism to our threat platform in the cloud. Meaning you will point all log sources to these sensors.
- Threat intelligence: The service uses an IP reputation data feed to identify the source of malicious activity and the feed is updated every 24 hours with the latest information available.
- Log data: We collect and correlate information from many log sources including Active Directory, critical servers, firewalls, and other assets that support syslog formatted transport. This log data is used to assist with investigation triage and can trigger customer alerts.
- Custom Alerts (learning loop): The service includes the ability to create customized alerts that allow us to optimize our threat detection and response for your specific network. Examples include events such as newly created Windows Admin Domains, account lockouts, notification of unwanted protocols being used, and more.
- Arctic Wolf Networks works with the client to perform monthly or on-demand internal & external vulnerability scans and will deliver the results of this report to your team for consideration.
- Arctic Wolf Networks operates a malware sandbox which is used, upon request, to analyze suspected files for malicious behavior.

SAVANT SOLUTIONS

ARCTIC WOLF

- Arctic Wolf Networks provides a customer portal to get information about the service we're performing along with reviewing 7 days of aggregated flow data (see diagram on next page).

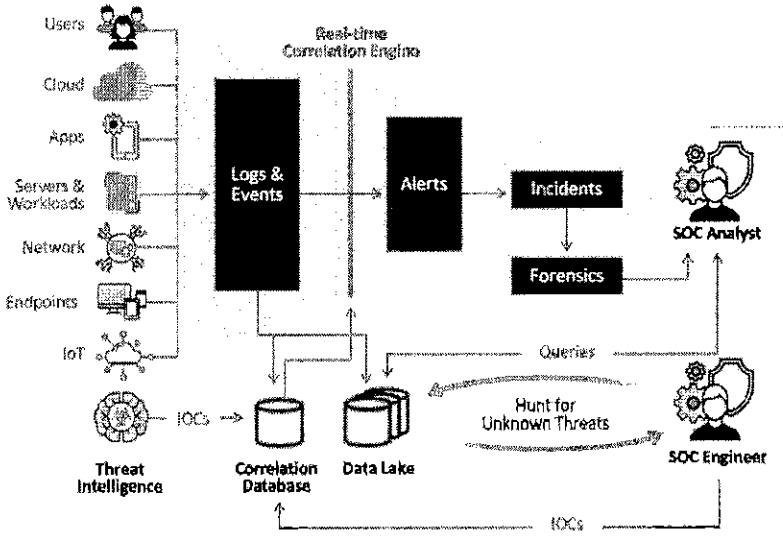
Client Portal – Dashboard



SAVANT SOLUTIONS

ARCTIC WOLF

High-level Diagram of Service



Average Customer Experience

- 165M Observations/Week
- 765 Investigations/Week
- 1-2 Incidents/Week

Real-time Correlation

- Analyze billions of events
- Real-time correlation against IOCs
- Reduced false positives

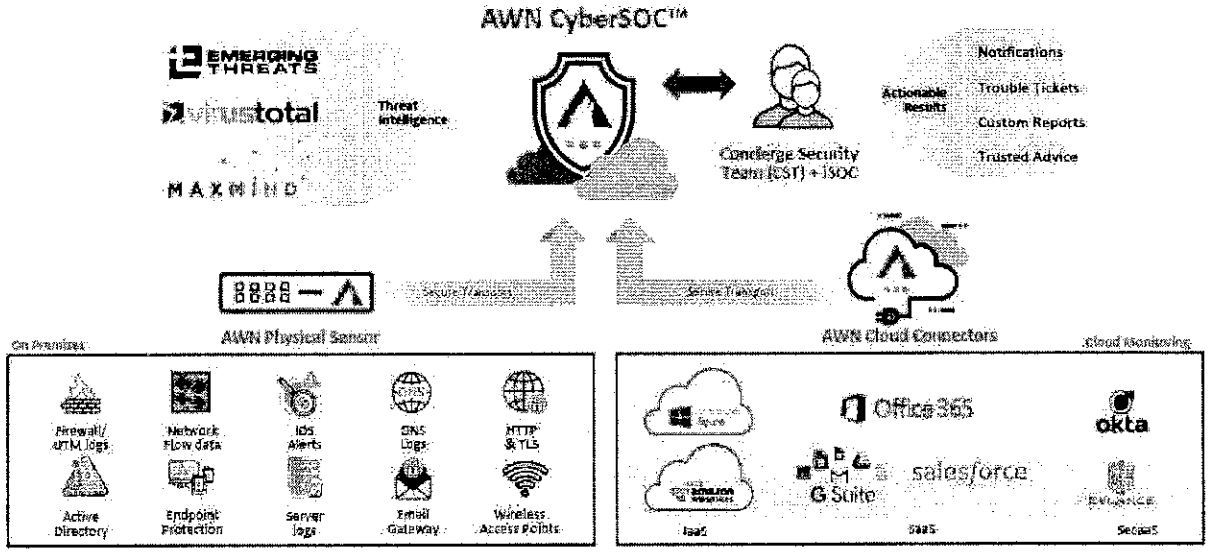
Forensics

- Search and research quickly
- Construct blast zone analysis and remediate

Hunt

- Hunt for unknown threats with deep analytics and machine learning
- Identify new IOCs to improve monitoring

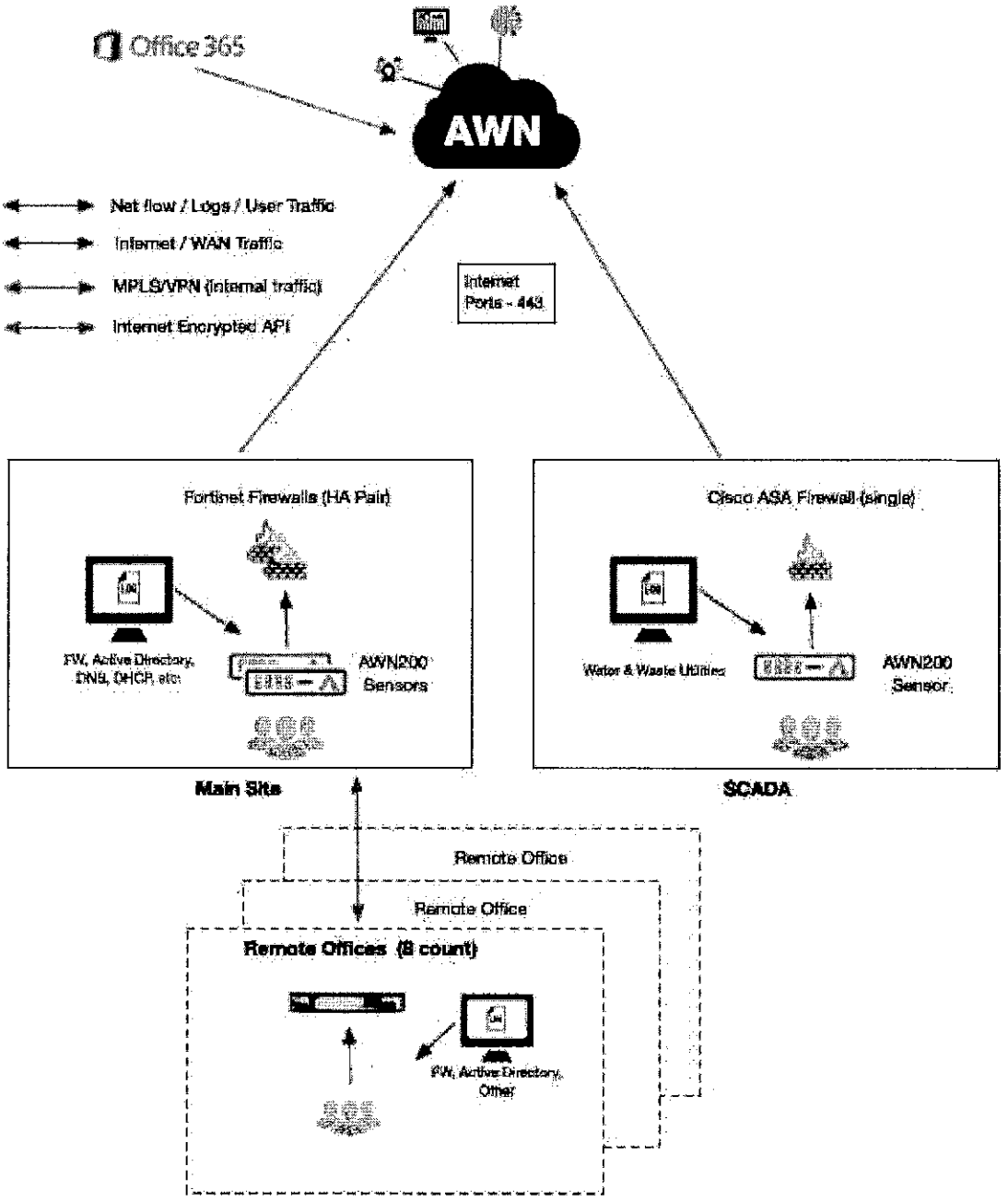
High-level Diagram of Technology Stack



SAVANT SOLUTIONS

ARCTIC WOLF

Architecture Diagram



SAVANT SOLUTIONS

ARCTIC WOLF

Typical Installation Cadence

Technical Kickoff
Technical Readiness

- Review contracts, establish timeline
- Define project plan and review SLAs
- Gather technical details

CyberSOC Essentials
Sensor Deployment and Log Setup

- Install sensors in primary location(s)
- Identify essential log sources
- Setup portal users and basic escalation

AWN CyberSOC Readiness
Finalize Onboarding

- Add remaining sensors and log sources
- Complete sensor installation for remote locations
- Configure external vulnerability scans to identify exposed services
- Validate that log sources are generating usable data

AWN CyberSOC Service Acceptance and Customization

- Introduce Concierge Security Team
- Review external vulnerability scan settings and fine-tune service
- Discuss any log source ingestion that would require security customization
- Identify your reporting and compliance needs
- Train customer portal users

SAVANT SOLUTIONS

ARCTIC WOLF

Unique Differentiators

Concierge Security Engineer

- Having a security expert that understands your business. No need to call into a tiered helpdesk line, you get a person who already knows you and your environment. In the heat of a security incident, time is saved by having a relationship already built with the Concierge Security Team.

Predictable & Easy Pricing Model

- Arctic Wolf Networks does not license by log volume, events per second, IDS Service or SIEM service, instance, or any other unquantifiable metric. The way we license is solely based on attack surface. It is an effort based model. Meaning you tell us how many users, how many servers, and we identify how many sensors are needed in the environment and then everything is included in the subscription rate. Everything we do is all included, there are no unexpected or hidden costs.
- The more logs we receive, the more visibility and context we can provide to enhance security.

AWN owns the solution

- Arctic Wolf Networks is not reliant on a third party SIEM product to perform our services. We have built our security platform for our Security Engineers. This gives us the ability to control our own destiny, which in the long run is beneficial for our customers.
- We believe that technology (e.g., machine learning) is valuable and very important to make humans efficient. We believe that humans will always be part of the security landscape. Coupling the two together brings a holistic approach to the managed detection and response marketplace and makes incident detection & response effective.
- Our solution is built in a way that we leverage "robots" for the tasks that make sense, but always with a human understanding and feeding these "learning loops." The way our service is setup is to customize the outcome for each customer. We can eliminate redundant alerts, we can customize incidents/alerts for any log source we collect, and ultimately we will have a hybrid of machine learning and human intelligence to make sure we eliminate noise and find the actionable intelligence within your network

SAVANT SOLUTIONS

ARCTIC WOLF

environment.

Required Log Source Support

Log Source	Transport Method	Notes
ARCTIC WOLF	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
amazon	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]

SAVANT SOLUTIONS

ARCTIC WOLF

Compliance

Please see the included documents that explain our compliance with the following:

- NIST 800-171 (included)
- PCI-DSS (included)
- Arctic Wolf has Security Operation Centers located in Provo, UT and Waterloo, Ontario, CA. We are SSAE16, SOC2 Type II, and ISO27001 compliant. To supply these certifications we would need an NDA in place with the City of San Clemente.

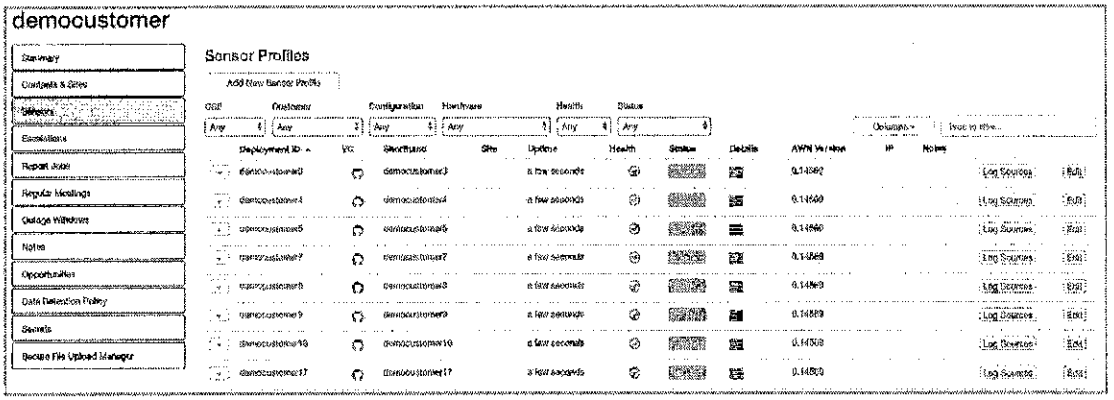
Contract SLA Response Time

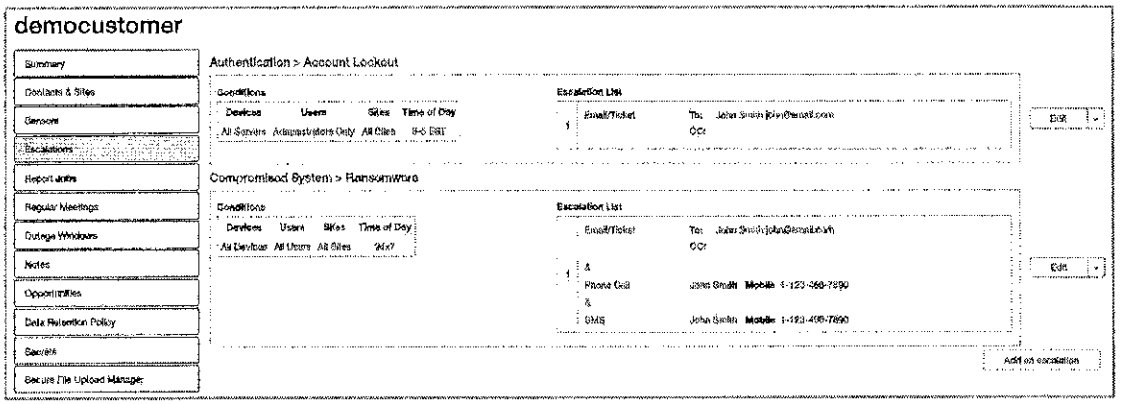
Security Engineers are available 24 hours a day seven days a week, including holidays. Customers can schedule specific activities with their Security Engineer by contacting Arctic Wolf at security@arcticwolf.com. Arctic Wolf will acknowledge any ticket submitted to security@arcticwolf.com within 1 Business Hour and will respond or provide an estimate of response determined by scope, size, and urgency. Security Incidents identified by Arctic Wolf to be Emergency will be escalated to the customer 24x7 within 30 minutes of discovery. The Customer and Arctic Wolf will need to define what constitutes an Emergency Incident but will typically include Ransomware.

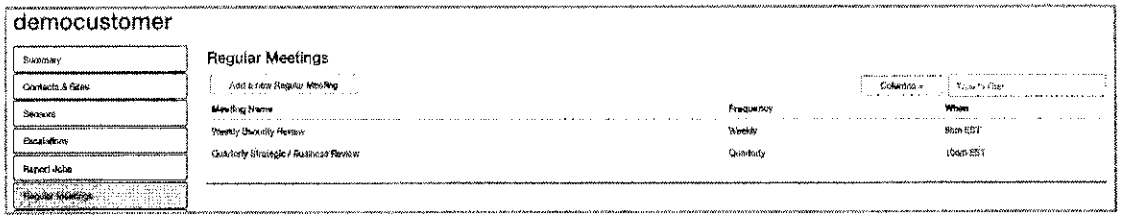
Any Emergency tickets should be escalated to Arctic Wolf by calling 888-272-8429 option 2. The Customer should state this is an emergency and Arctic Wolf will respond within 5 minutes 24x7. Arctic Wolf will notify and escalate to customer any security events in a timely manner but no more than 2 hours after discovery. Typical notification is through e-mail by a trouble ticket, but customer can request special notification through phone or other means if supported. Arctic Wolf and customer will agree on notification and escalation of security incidents. Notifications will include a description of the security event, the level of exposure, and a suggested remediation strategy.

We setup and make sure the escalation chain for specific incidents are documented ahead of time. Below is a look into our customer directory where we store workflow integration and

customer configurations (all integrated into our platform and workflow). This means when a security engineer needs to escalate a security incident the escalation process is part of that.







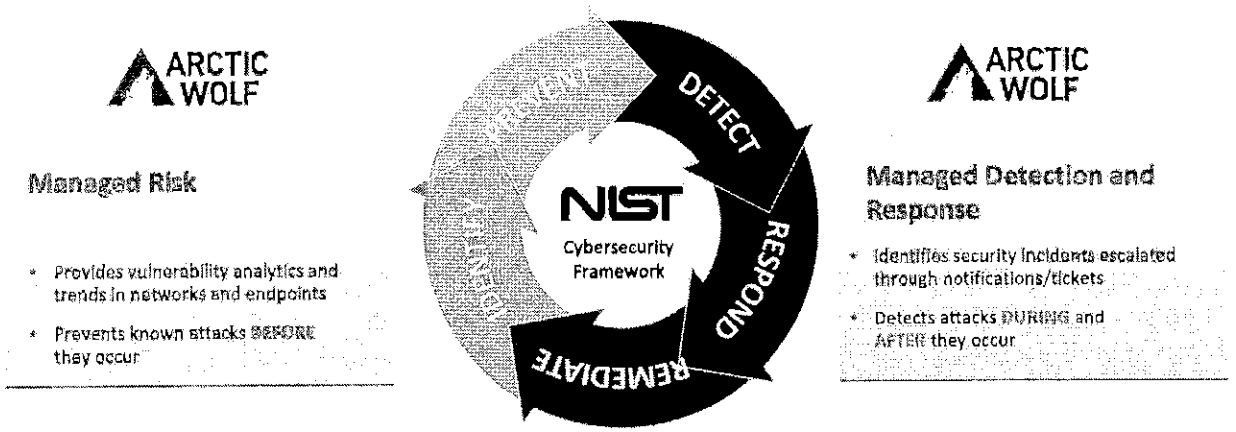
SAVANT SOLUTIONS

ARCTIC WOLF

Optional Services

Arctic Wolf Managed Risk Services Overview

The Managed Risk portfolio of Arctic Wolf's risk assessment services enables you to continuously scan your networks and endpoints, and quantify risk-based vulnerabilities. Unlike alternatives that rely on automated approaches that make assessing vulnerabilities difficult, Arctic Wolf's Concierge Security Team™ provides a quantified, real-time understanding of your cyber risks so you can take prioritized action to improve your cyber risk posture. It complements Arctic Wolf Managed Detection and Response™, which provides the most comprehensive security operations center (SOC)-as-a-service in the industry.



Managed Risk provides the following services:

Dynamic Asset Identification: Automatic and continuous profiling and classification of your network assets to build a comprehensive inventory.

Continuous Risk Scanning: Ongoing scans rather than occasional ones to avoid risky delays in security awareness.

Comprehensive Risk Profiling: Aggregates and quantifies risk indicators from Managed Risk, which are weighted based on the industry standard CVSS (Common Vulnerability Scoring System).

SAVANT SOLUTIONS

ARCTIC WOLF

External/Internal Network Scanning: Identifies vulnerabilities that could be exploited in internet-facing and internal systems on the network;

Host-Based Risk Assessment: Host-based agents monitor hardware and software, and registry configurations and changes to reveal risks that can only be detected through on-device observations.

Dark Web Scan: Our external scan will also scan against dark websites such as shodan.io and credentials storing databases and let you know if we find your assets on the dark web.

Managed Risk Vulnerability Scanning

Managed Risk includes the Continuous Network Scanner portion of the portfolio. It provides External and internal vulnerability assessment tools that discover IP-connected devices, look for vulnerabilities resulting from outdated software, and prioritize your patch strategy.

- External Vulnerabilty Scans: scans internet-facing servers to understand your company's digital footprint.
- Key features include:
  - Continuous scanning of external-facing assets.
  - Proactive Risk Monitoring
  - Webserver Scans
  - Automated sub-domain detection
  - Darkweb Scans
- Internal Vulnerability Scans: continuously scans all of your internal IP-connected devices, cataloging your core infrastructure, equipment/peripherals, workstations, internet of things (IoT) and personal (i.e. BYOD) devices.
- Key Features include:
  - Continuous scanning of internal assets
  - Dynamic asset identification and classification
  - Webserver scans
  - Automatic updates
  - Stateless scanning and secure transfers

SAVANT SOLUTIONS

ARCTIC WOLF

Managed Risk Agent

Managed Risk Agent is the Continuous Host-Based Risk Assessment tool provided in the portfolio. Managed Risk Agent is a turnkey social engineering simulator that tests the cyber hygiene of your employees and measures your organization's susceptibility to phishing emails, SMS messages, and voice calls. Key Features Include:

- Agent Based – Windows server/workstations, MacOS
- Proactive Risk Monitoring
- Audit Reporting
- Host Based IVA Scanning
- CIS Benchmarking/Base-lining

Managed Risk – Concierge Services

- Monthly Risk Review
- Quarterly risk roll-up and progress tracking
- Tickets and alerts from AWN CyberSOC
- Classification and organization of assets and risks
- Risk discovery and validation
- Sensor configuration and monitoring

Managed Risk Dashboard

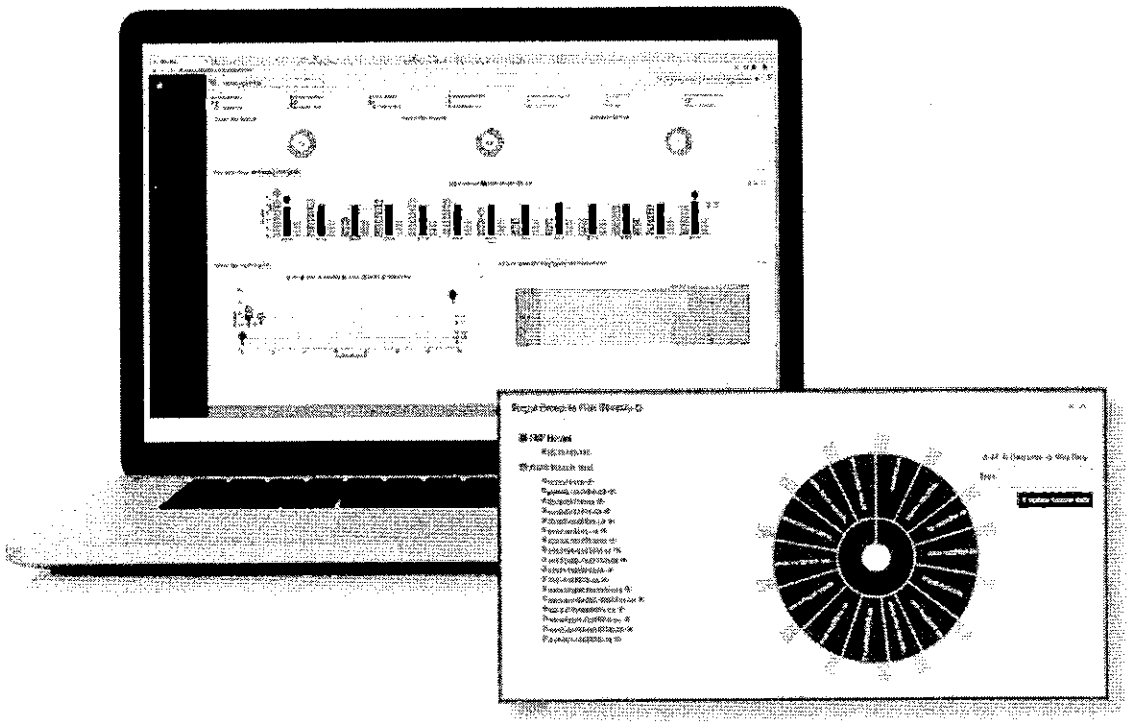
A cloud-based dashboard that provides visibility into continuous cyber risk assessment by incorporating all meaningful cyber risk indicators from your business. It identifies the highest-priority issues and alerts you to emerging risks before they evolve into real problems. The Managed Risk Dashboard empowers you to take meaningful, efficient action by using these key features:

- Comprehensive risk profiling
- Informative user interface
- Proactive notification and alerts
- Advanced threat data analysis
- Actionable reporting
- API Integrations

SAVANT SOLUTIONS

ARCTIC WOLF

- Crowd-sourced templates
- Intelligent landing pages



Penetration Testing

All penetration tests are being delivered in accordance with the following industry standards and framework methodologies:

- ISO 27001
- ISO 9001
- Offensive Security
- Pentest-Standard.org
- EC Council CEH and LPT
- OWASP
- UK CREST

SAVANT SOLUTIONS

ARCTIC WOLF

- US CNSS 4011 and 4013

Our vulnerability assessment methodology encompasses a multitude of tools and skills to assess the overall health of a company's security infrastructure. As such, all security assessments must adapt to an organization's infrastructure, host services, and security policies so as to provide a holistic security review of their networked environment. Our methodology is based around 4 key phases:

Phase 1 – Scoping

This is the first phase of our Infrastructure Security Test and it is carried out before any technology-based assessments take place. In this phase, we fully discuss the clients' requirements and defines a test strategy for the Vulnerability Assessment / Penetration Test (Black box, White box, Grey box). GigIT attempts to understand where the client's perceived risk and threat emanates from. (Internal, External, Web App). In all instances, we will conduct a face to face or telephone based scoping exercise that is run by both an Account Manager and a Security Consultant.

We use the information collected at this phase to generate a formal proposal (i.e. this document), targeted to the clients' individual requirements. This will detail our approach to security testing as well as the scope of the testing engagement.

Phase 2 – Reconnaissance and enumeration

We will conduct passive network sniffing to capture broadcast and multicast data that is available across the network. We will investigate network protocols such as CDP, VTP, OSPF, HSRP and VRRP traffic where applicable.

We will identify non-network devices that are issuing broadcast and multicast traffic. This will frequently include DHCP, BootP and NetBIOS over IP packets that can be used to identify resource topology.

We will investigate Application protocols such as DNS, LDAP, SNMP, Finger, RPC, SMTP, NIS, NFS and SMB. As part of this phase, we will identify which resources will be in-scope by network location and resource interconnectivity.

SAVANT SOLUTIONS

ARCTIC WOLF

We will build a topology form for all resources that are in-scope for the Vulnerability Assessment / Penetration Test. This topology will consist of MAC addresses, IP addresses, hostnames, and resource type classifications. The topology form will be discussed with the client to ensure that it is consistent with their Test requirements. Any systems that are believed to be out-of-scope will be discussed with the client to ascertain whether they should truly be out of scope, or brought in to scope of the Security Test.

Phase 3 – Mapping and Service identification

All tests commence with a sweep that is designed to identify network and system resources available within the environment. At a network level, this will initially involve both active and passive TCP/UDP/ICMP scanning, ARP scanning, routing assessment,

VLAN assessment and network ingress/egress point classification. In relevant scenarios, we will provide additional service identification exercises based on parameters captured at Phase 1.
This may include, IPV6 service identification, IPX/Appletalk identification and other IP based service identification that make use of IP protocol types. (GRE/ESP/AH etc.)

Following the initial service identification, we will attempt to identify the application protocol that is in use and the vendor and version of the software that is providing that application. This will be accomplished using a combination of protocol fingerprinting, banner grabbing, and manual communication with the service itself.

Phase 4 – Vulnerability and Exposure Analysis

Each port, service and application identified in Phase 3 will be reviewed for vulnerabilities. This assessment will identify publicly known vulnerabilities in application code, as well as configuration and deployment vulnerabilities that have been introduced in to the environment by the client. We will blend information from both of those elements together to provide a thorough vulnerability assessment of the environment.

Our consultants are skilled security professionals that are capable of identifying vulnerabilities and exposures in custom applications. Through a combination of fuzzing techniques along with our security consultant's understanding of application coding, it is possible to identify application code vulnerabilities at this level that have not been previously identified.

SAVANT SOLUTIONS

ARCTIC WOLF

Network Penetration Testing Methodology (for Network Pen Test Services only)

In addition to the phases outlined under Vulnerability Assessment Methodology, the following 2 additional phases are executed during a penetration test:

Phase 5 – Service Exploitation

During Phase 5, we will attempt to actively exploit vulnerabilities and misconfigurations identified at Phase 4. Exploitation can include a number of different types of tasks, depending on the vulnerability and misconfiguration identified within a system or application. In all instances, GigIT discusses the options for exploitation with the client prior to the commencement of the test. Exploitation tasks may include some or all of the following types of activities:

- Password Guessing & Password reuse
- Authentication bypass to gain access to system resources
- Buffer Overflow attacks
- Issuing local/remote commands to a system to escalate privileges
- Sending Exploit code to a vulnerable process, application, or daemon
- Active Man In The Middle attacks
- Taking advantage of misconfiguration

The Exploitation Phase is used to validate vulnerabilities in Phase 4 assessments. As a consequence, it is a mechanism that can eliminate false positives from incorrectly being identified. In addition to this, Phase 5 provides a more active security assessment of a client's infrastructure and application environment.

Phase 6 – Pivoting

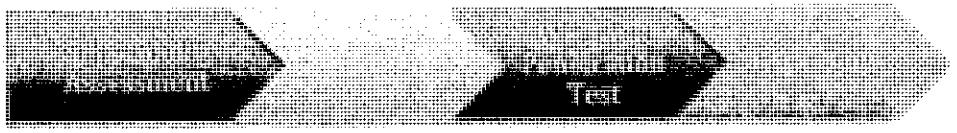
Once we have exploited a device, our Security Consultant will look to pivot through this device and start enumerating other parts of the environment that ordinarily might not be directly accessible. We will take credentials from one system and attempt to reuse them in other systems. The aim of this phase is to gain access to as many devices as possible and identify as many security exposures as possible across the IT estate.

The pivoting phase takes advantage of the trust relationship between systems, including SSO mechanisms, shared system/super-user passwords, and Active Directory based resource manipulation.

SAVANT SOLUTIONS

ARCTIC WOLF

During a final phase, we document all vulnerabilities and exposures within the environment (common to all included services). Any vulnerability, exposure or point of exploitation is thoroughly assessed before it is written up. Reports aim to quantify the exposures and identify how and why they may pose risks to the business. Remediation advice and guidance is provided in our report on how the environment should be improved. Debriefs can either take place via conference call, through WebEx, or through face-to-face meetings. During these debrief sessions, we will walk the client through their security exposures and offer advice and guidance on how the environment should be improved.



Deliverables

Upon completion of the security evaluation, the Project Manager will assemble the deliverables and the client will be provided with a detailed report. This report consists of two parts, a Management Summary and a Technical Report, and will be provided to the client one week after completion of the security assessment.

Master Report

The master report contains 2 subsets of reports in 1 document.

Management Summary Report
The Management Report gives a non-technical, clear and precise image on the business impact of the attack. By reading the report the management will be able to clearly understand the operational IT risks affecting their business, and to plan a cost- and time-efficient process of security improvement, in order to minimize the identified risks in the shortest terms.

The Management Report includes:

Non-technical list of discovered threats and risks, and their impact on the client's business processes, ordered by priority and importance
Proposed solutions with approximate timing and pricing

Technical Report

SAVANT SOLUTIONS

ARCTIC WOLF

The Technical Report is designed for the client's technical staff, and is actually a series or reports based upon the services performed. The main purpose of the report is to show strengths and weaknesses of the client's IT infrastructure, and to advise how to improve the security of it. The Technical report also enables the technical staff to become more familiar with the attack scenarios that hackers would use for attacking their infrastructure, in order to be able to prevent them in the future.

Technical Reports include:

- Description of methodologies and approaches used
- Detailed technical description of vulnerabilities and weaknesses discovered
- Detailed technical description of positive security aspects identified
- Solutions to patch the vulnerabilities and prevent them in future

Results Debrief

Debriefs take place via a conference call, through GoToMeeting / WebEx. During these debrief sessions, we will walk the client through their security exposures and offer advice and guidance on how the environment should be improved. Where possible, we will provide tangible examples of what vulnerabilities exist, how an attacker could exploit them, and what data assets can be compromised. We will also provide recommendations on how individual exposures can be fixed, as well as higher-level guidance on Security Policy, procedure, topology, SDLC and other factors that could be relevant to improving the client's security posture.

3. *Project Scope*

The following sections describe the Services in greater detail and identify City of San Clemente and Arctic Wolf Networks responsibilities necessary for completion of the onboarding engagement.

3.1 Environment - Servers / Users

Category	Quantity / Time Frame
Knowledge Workers	350
Office 365	350
Managed Detection Data Storage	1 Year
Servers	62

3.2 Environment Architecture

Sites	Sensors/Scanners
Main Site – Managed Detection Sensors	AWN-201 (2)
Main Site - Virtual Scanner	ESXi VM (1)

3.3 Managed Detection and Managed Risk Onboarding

3.3.1 Technical Kickoff

- City of San Clemente to complete the onboarding document for all sensors and scanners.
- AWN will gather and confirm basic information to:
  - Provision and ship the sensors and scanners as well as customize preferences
  - Contacts
  - Escalation and Incident Workflow process
  - Additional log source identification
  - Network segmentation information
  - Critical Services, Devices, Users and Groups, and Segments AWN should be aware of.

3.3.2 Sensor / Scanner Provisioning / Shipment

- AWN will use the information from the technical meeting and onboarding form to get the sensor(s) provisioned and shipped to City of San Clemente.
  - The AWN Onboarding form will be provided within the Welcome ticket after order execution

3.3.3 Managed Detection Sensor Installation

- City of San Clemente will perform a cabling exercise to get the sensors installed at each of the locations. AWN will direct City of San Clemente through this process remotely. If the deployment method is SPAN/Mirror, City of San Clemente will be required to provide a SPAN/Mirror port. Sensor installation documents can be reviewed here: Sensor Setup
- City of San Clemente will make sure any firewall/proxy configurations are made to allow the sensor(s) to communicate with the AWN cloud (see onboarding document for details)
- AWN will validate that sensor(s) are communicating properly with AWN Cloud

3.3.4 Risk Scanner Installation

- City of San Clemente will provision an ESXi virtual machine per Arctic Wolf specifications. AWN will direct City of San Clemente through the AWN virtual machine setup process remotely.
- AWN will configure and register Risk scanner remotely with City of San Clemente.
- City of San Clemente will make sure any firewall/proxy configurations are made to allow the scanner(s) to communicate with the AWN cloud (see onboarding document for details)

3.3.5 Essentials Phase

- Preliminary Sensor Configuration
    - Initial sensor installation and verification at primary locations
    - Configure Service for the following log sources
        - Firewalls
        - Active Directory Services
        - Domain Controllers
        - DHCP
        - SaaS apps (if applicable)
    - Customer portal preparation
- Risk Scanner Configuration
    - Initial scanner virtual machine setup and initial scanner configuration
        - Configure local network subnet scan and scan schedule

3.3.6 Readiness Phase

- Follow on Configuration
  - Complete sensor installations for sites in-scope for onboarding
  - Configure additional log sources
  - Configure external exposure scanning systems
  - Risk scanner verification of connectivity and scan data in AWN Cloud

3.3.7 Service Acceptance and Customization

- Introduction of Concierge Security Team
- Discuss log source ingestion that would require security customization
- Discuss Risk scanner connectivity and registration
- Validate report delivery
- Identify reporting and compliance needs
- Train customer portal users

3.4 Managed Detection and Managed Risk Ongoing Services

- Collect appropriate (as agreed to by customer) log data and store for agreed period with customer (default is 90 days but can be tailored to your requirements: 1 day to 7 years)
- Typical data sources: AWN Sensors, firewall logs, server logs, network device logs, other security devices, and DNS logs
- Regular continuous review of data flows and output of machine analyties to find breaches, vulnerabilities and risky behaviors
- Report security incidents to customer in the manner the customer prescribes (e.g., email, text, phone call, or a phone escalation tree)
- For each incident prescribe a recommended remediation plan
- Produce regular monthly and quarterly summaries as agreed with customer
- Monthly vulnerability assessment of external facing corporate infrastructure to identify any external risks
- Respond to ad-hoc queries for clarification or further analysis of questions about security issues
- Quarterly review meeting with prioritized recommendation to improve security posture and reduce risk
- Forensic and malware analysis support when requested and as required to remediate or do root cause analysis of breaches

3.5 City of San Clemente Responsibilities

Arctic Wolf Networks acknowledges that its timely provision of and access to, facilities, equipment, assistance, cooperation, complete and accurate information and data from Arctic Wolf Networks departments, (including such systems and networks required for functional testing). City of San Clemente acknowledges that Arctic Wolf Networks' ability to perform the Services depends upon City of San Clemente fulfillment of these obligations. Other City of San Clemente responsibilities include:

- Network administration
- Firewall administration
- Server administration
- Arctic Wolf Agent deployment to intended endpoints

3.6 Mutual Responsibilities

In support of the Services provided hereunder, both City of San Clemente and Arctic Wolf Networks shall:

- Conduct project review meetings at a mutually agreed upon time and location to discuss the project status, issues, new requirements and overall project satisfaction.
- Support and provide representation at these meetings, which will cover status update, schedule update, pending changes, open issues and action items.
- Meet at the conclusion of this project to bring to closure the project and capture, discuss and resolve any project issues that may have arisen.

3.7 Assumptions and Timeline

Below is a high-level timeline example for the onboarding project:

Task	Finish Date
Technical Review Meeting	Scheduled following receipt of order and after receiving completed Onboarding forms
Sensor(s) delivery	5 – 10 business days from Technical Meeting
Sensor/scanner staging and installation	Varied, depending on customer schedule
Essential log source configuration	~ 1 day per location
Cloud Services setup	~ 1 to 2 hours per cloud application
Additional log sources	Varied, depending on type/amount
Validation of Onboarding configuration	~ 1 day
Open Production AWN service / Introduce CST	1 hour meeting

3.8 Out of Scope

Arctic Wolf Networks is responsible for performing only the Services described in this document. All other services are considered outside the scope of this document. If City of San Clemente wishes to modify the Services, City of San Clemente and Arctic Wolf Networks will define and scope those requirements and follow standard change control procedures.

3.9 Location

The onboarding services will be delivered using Arctic Wolf Networks standard delivery model, which will be remote/offsite delivery. If City of San Clemente requires a different delivery model, the fees, expenses, scope of work and/or Deliverables specified herein are subject to modification in accordance with standard change control procedures.

4. *Resources*

4.1.1 Project Team

Arctic Wolf Networks recommends that City of San Clemente plan for availability of the following resources:

Security Team Resource

Network / Firewall Resource

Active Directory Resource

Arctic Wolf Networks will assign a project team that will include the following resources:

Project Manager

Professional Services Engineer

4.2 Change Procedures

4.2.1 Process

Any request for any change in Services must be in writing; this includes requests for changes in project plans, scope, specifications, schedule, designs, requirements, service deliverables, software environment or any other aspect of this document. Arctic Wolf Networks shall not be obligated to perform tasks related to changes in time, scope, cost, or contractual obligations until City of San Clemente and Arctic Wolf Networks agree in writing to the proposed change.

5. *Reporting Status*

5.1 Progress Reports

Arctic Wolf Networks will hold regularly scheduled status meeting with City of San Clemente and will provide follow up meeting status documentation following each status meeting.

SAVANT SOLUTIONS
Your Trusted IT Advisor

1007 7th St, 5th Floor
Sacramento, CA 95814
(916) 836-8182
sales@savantsolutions.net

Quote# BB-010920-3

Date: 1/9/20
Terms: NET30
FOB: Destination
Valid for: 30 days
Shipping: Ground

Bill To
City of San Clemente
Attn: Accounts Payable
100 Avenida Presidio
San Clemente, CA 92672
Phone:

Ship To
City of San Clemente
Attn: Brian Brower
100 Avenida Presidio
San Clemente, CA 92672
Phone:

Line #	Part No.	Description	Qty.	Unit Price	Ext. Price
1	AW-MDR-USER	Arctic Wolf MDR user license - 310 users	1	$87,900.00	$87,900.00
2	AW-MDR-SE	Arctic Wolf MDR server license	62	$195.00	$12,090.00
3	AW-MDR-1Y	Arctic Wolf MDR Log 1 YR Retention	1	$5,467.00	$5,467.00
4	AW-MDR-2XX-S	AWN 200 Series Sensor	2	$4,000.00	$8,000.00
5	AW-MDRO365	Arctic Wolf MDR Office 365 user license	350	$38.00	$13,300.00
6	AW-MDR-OB	Arctic Wolf MDR Onboarding (One time fee)	1	$2,100.00	$2,100.00
7	AW-MR-U	Arctic Wolf Managed Risk 300 Users	1	$24,000.00	$24,000.00
8	AW-MR-SE	Arctic Wolf Managed Risk server license	62	$54.00	$3,348.00
9	AW-MR-OB	Arctic Wolf Managed Risk Onboarding (One time fee)	1	$500.00	$500.00
			Total:		$156,705.00
			Tax:		$0.00
			Credit:		$0.00
			Shipping:		$240.00
			Total:		$156,945.00

Notes: 3 Year Contract with MDR and MR

Thank you for giving Savant Solutions the opportunity to support you!
Each order helps supports a non-profit in need.

www.SavantSolutions.net

Payment Terms:

Total 3-year cost of Purchase, Implementation, and Arctic Wolf Services Services is $156,945.

Payments will be made by the Customer to Savant Solutions based on the following schedule:

Year 1: Upon contract execution and prior to onboarding: $54,208.33
Year 2: Prior to the beginning of the year 2 service period: $51,368.33
Year 3: Prior to the beginning of the year 3 service period: $51,368.33

SAVANT SOLUTIONS
Your Trusted IT Advisor

1007 7th St, 5th Floor
Sacramento, CA 95814
(916) 836-8182
sales@savantsolutions.net

Quote# BB-031220-1

Date: 0312/20
Terms: NET30
FOB: Destination
Valid for: 30 days
Shipping: Ground

Bill To
City of San Clemente
Attn: Accounts Payable
100 Avenida Presidio
San Clemente, CA 92672
Phone:

Ship To
City of San Clemente
Attn: Brian Brower
100 Avenida Presidio
San Clemente, CA 92672
Phone:

Line #	Part No.	Description	Qty	Unit Price	Est. Price
1	PEN-TEST-PROSERV	Penetration Testing Professional Services Per IP	38	$500.00	$19,000.00
2	VUL-SCAN	Vulnerability Scanning for up to 100 IP's	1	$6,000.00	$6,000.00
					$0.00
					$0.00
					$0.00
					$0.00
					$0.00
					$0.00
					$0.00
			Total		$25,000.00
			Tax		$0.00
			Credit		$0.00
			Shipping		$0.00
			Total		$25,000.00

Notes: All work will be done remote via VPN or travel and expenses will need to be added. Work is expected to take between 2-3 weeks.

Thank you for giving Savant Solutions the opportunity to support you!
Each order helps supports a non-profit in need.

www.SavantSolutions.net

Payment Terms:

Total cost of Penetration Test and Vulnerability Assessment is $25,000. Payments will be made in full by the Customer to Savant Solutions upon completion of the engagement and all deliverables identified in this agreement.

EXHIBIT "B"

SCHEDULE OF PERFORMANCE

Work shall be performed according to the target milestone timeline below.

Timelines may change based on mutual agreement between City and Contractor.

ArcticWolf Network Implementation	
Project Kick-off	1 week from contract execution date.
Sensors delivered and installed	1 week from project kickoff
Cloud Services setup/ Log source configuration	1-2 weeks from sensor delivery
Validation of onboarding configuration	2 weeks from setup and configuration
Open Production AWN service / Introduce CST	3 weeks from project kick off
Implementation Total	3 weeks from contract execution

Vulnerability Assessment and Penetration Test	
Automated Vulnerability Scanning – 100 IP's	Begin 1 week from receipt of Purchase Order. Duration: 5 Business Days
Manual Pen Test for 38 IP's	Begin 1 week from receipt of Purchase Order. Duration 15 Business Days

[See 1.3 of Agreement]

WORKER'S COMPENSATION INSURANCE CERTIFICATION

Project No. _____

WORKERS' COMPENSATION DECLARATION

I hereby affirm under penalty of perjury one of the following declarations:

(ONE OF THE BOXES BELOW MUST BE CHECKED)

☐ I have and will maintain a certificate of consent from the California Labor Commission to self-insure for workers' compensation, as provided for by Section 3700 of the Labor Code, for the performance of the work to be performed under this contract.

☑ I have and will maintain workers' compensation insurance, as required by Section 3700 of the Labor Code, for the performance of the work to be performed under this contract. My workers' compensation insurance carrier and policy number are:

Carrier Sentinel Insurance Company

Policy Number 46 WEC AS9039

☐ I certify that, in the performance of the work under this Agreement, I shall not employ any person in any manner so as to become subject to the workers' compensation laws of California, and I hereby agree to indemnify, defend, and hold harmless the City of San Clemente and all of its officials, employees, and agents from and against any and all claims, liabilities, and losses relating to personal injury or death, economic losses, and property damage arising out of my failure to provide such worker's compensation insurance. I further agree that, if I should become subject to the workers' compensation provisions of Section 3700 of the Labor Code, I shall forthwith comply with those provisions.

WARNING: FAILURE TO SECURE WORKERS' COMPENSATION COVERAGE IS UNLAWFUL, AND SHALL SUBJECT AN EMPLOYER TO CRIMINAL PENALTIES AND CIVIL FINES UP TO ONE HUNDRED THOUSAND DOLLARS ($100,000), IN ADDITION TO THE COST OF COMPENSATION, DAMAGES AS PROVIDED FOR IN SECTION 3706 OF THE LABOR CODE, INTEREST, AND ATTORNEY'S FEES.

882/062266-0001
773382.08 a04/22/20

Workermans'
Comp

Dated: April 24, 20 20

Savant Solutions, Inc.

Contracting Firm

By: Caleb Kwong

Caleb Kwong

Title

CEO

Address

1007 7th St, 5th Floor, Sacramento, CA 95814

SAVANT SOLUTIONS
Your Trusted IT Advisor

1030 G St.
Sacramento, CA 95814
(916) 836-8182
sales@savantsolutions.net

Quote# BB-051623-1

Date: 5/16/23
Terms: NET30
FOB: Destination
Valid for: 30 days
Shipping: Ground

Bill To

City of San Clemente
Attn: Accounts Payable
100 Avenida Presidio
San Clemente, CA 92672
Phone:

Ship To

City of San Clemente
Attn: Brian Brower
100 Avenida Presidio
San Clemente, CA 92672
Phone:

Line #	Part No.	Description	Qty	Unit Price	Ext. Price
1	AW-MDR-USER	Arctic Wolf MDR user license - 310 users	310	$103.00	$31,930.00
2	AW-MDR-SE	Arctic Wolf MDR server license	62	$70.00	$4,340.00
3	AW-MDR-1Y	Arctic Wolf MDR Log 1 YR Retention	1	$1,968.00	$1,968.00
4	AW-MDR-2XX-S	AWN 200 Series Sensor	2	$1,440.00	$2,880.00
5	AW-MDRO365	Arctic Wolf MDR Office 365 user license	350	$13.68	$4,788.00
6	AW-MR-U	Arctic Wolf Managed Risk 300 Users	310	$34.83	$10,797.30
7	AW-MR-SE	Arctic Wolf Managed Risk server license	62	$19.44	$1,205.28
		Year 2 - $60,804			
		TCO of 2 years = $118,712.58			

Notes: 2 Year Contract with MDR and MR
5% increase on all line items each year

Total:		$57,908.58
Tax:		$0.00
Credit:		$0.00
Shipping:		$0.00
Total:		$57,908.58

Thank you for giving Savant Solutions the opportunity to support you!
Each order helps supports a non-profit in need.

www.SavantSolutions.net

RESOLUTION NO. 23-36

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF SAN CLEMENTE, CALIFORNIA, AUTHORIZING THE CITY MANAGER TO EXECUTE A FIRST AMENDMENT TO A PROFESSIONAL SERVICES AGREEMENT TO SAVANT SOLUTIONS, INC. TO PROVIDE MANAGED SECURITY SERVICES

WHEREAS, the City wishes to ensure the City's computer network and cyber defense mechanisms are actively monitored for attacks or malicious activity, and critical Information Technology assets are protected from such activities; and

WHEREAS, the City has contracted for professional managed security services under a Professional Services Agreement (Attachment 1) with Savant Solutions for the past three years; and

WHEREAS, the Professional Services Agreement (Attachment 1) expires on July 1, 2023; and

WHEREAS, the City has received a proposal for two years of additional service from Savant Solutions, Inc with an annual cost of $57,909 in year one and $60,804 in year two for a two-year total of $118,713.

NOW, THEREFORE, the City Council of the City of San Clemente does hereby find, determine and resolve as follows:

SECTION 1. That the above recitations are true and correct and incorporated herein.

SECTION 2. That the City Manager is authorized to execute the First Amendment to the Professional Services Agreement for Managed Security Services with Savant Solutions, Inc. in an amount not to exceed $300,658, which includes an additional $118,713 for the two year extension of the Arctic Wolf Networks Managed Detection and Response and Managed Risk Services through July 1, 2025 in a form substantially similar to the agreement attached to this resolution as Exhibit 1 and incorporated fully herein by this reference.

SECTION 3. That the City Clerk shall certify to the passage and adoption of this resolution and enter it into the book of original resolutions.

PASSED AND ADOPTED this _____ day of June, 2023.

_____
Mayor of the City of
San Clemente, California

ATTEST:

_____
CITY CLERK of the City of
San Clemente, California

STATE OF CALIFORNIA)
COUNTY OF ORANGE) §
CITY OF SAN CLEMENTE)

I, LAURA CAMPAGNOLO, City Clerk of the City of San Clemente, California, do hereby certify that Resolution No. _23-36 was adopted at a regular meeting of the City Council of the City of San Clemente held on _____ day of June 2023, by the following vote:

AYES:

NOES:

ABSENT:

_____
CITY CLERK of the City of
San Clemente, California

Approved as to form:

_____
Elizabeth A. Mitchell, City Attorney

FIRST AMENDMENT TO PROFESSIONAL SERVICES AGREEMENT FOR MANAGED SECURITY SERVICES

This First Amendment to Professional Services Agreement for Managed Security Services (this "First Amendment") is made and entered into on this _____ day of _____, 2023, by and between the CITY OF SAN CLEMENTE, a California municipal corporation ("City"), and Savant Solutions, Inc., a Wyoming corporation, of 1030 G Street, Sacramento, California 95814 ("Contractor").

R E C I T A L S:

A. City and Contractor entered into that certain Professional Services Agreement for Managed Security Services (the "Agreement") dated April 21, 2020;

B. City and Contractor desire to amend the Agreement in the manner provided herein.

C O V E N A N T S:

City and Contractor, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, agree as follows:

Section 1: Section 1.1 (Term) of the Agreement is hereby amended to be extended for two (2) years until July 1, 2025, unless terminated earlier pursuant to the terms of the Agreement.

Section 2: Section 3.1 of the Agreement is hereby amended to increase the total compensation under the Agreement from One Hundred and Eighty One Thousand, Nine Hundred and Forty Five Dollars ($181,945) to Three Hundred Thousand Six Hundred and Fifty Eight Dollars ($300,658).

Section 3: Section 5.2 of the Agreement is hereby amended to add paragraph D, which shall read as follows:

D. Cyber Liability Insurance with limits not less than $2,000,000 per occurrence or claim, $4,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Contractor in this agreement and shall include, but not be limited to, claims involving security breach, system failure, data recovery, business interruption, cyber extortion, social engineering, infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, and alteration of electronic information. The policy shall provide coverage for breach response costs, regulatory fines and penalties as well as credit monitoring expenses.

Section 4: Exhibit A to the Agreement is hereby amended to add that Contractor shall also perform those services described in Exhibit "A" to this First Amendment, which exhibit is attached hereto and incorporated herein by this reference, in addition to the services to be performed by Contractor as referenced in Exhibit A to the Agreement.

Section 5: Except as expressly amended by this First Amendment, the remaining portions of the Agreement shall remain in full force and effect.

IN WITNESS WHEREOF, the parties hereto have caused this First Amendment to be duly executed on the respective dates set forth opposite their signatures.

CITY OF SAN CLEMENTE

By:_____
Andy Hall, City Manager

ATTEST:

Dated: _____, 2023

_____
CITY CLERK of the City of
San Clemente, California

Approved as to form:

Savant Solutions, Inc., a Wyoming corporation ("CONTRACTOR")

_____
Elizabeth A. Mitchell, City Attorney

By:_____
Caleb Kwong, CEO, Secretary, CFO

Dated: _____, 2023

_____
Finance Authorization

EXHIBIT "A"

AW-MDR-USER Arctic Wolf MDR user license - 310 users
AW-MDR-SE Arctic Wolf MDR server license - 62 Servers
AW-MDR-1Y Arctic Wolf MDR Log 1 YR Retention
AW-MDR-2XX-S AWN 200 Series Sensor - 2
AW-MDRO365 Arctic Wolf MDR Office 365 user license 350 Mailboxes
AW-MR-U Arctic Wolf Managed Risk - 310 Users
AW-MR-SE Arctic Wolf Managed Risk server license - 62 Servers

Service Dates: July 1, 2023 through June 30, 2025