

CONSULTANT: Emagined Security, Inc.
CONTACT PERSON: David Sockol, CEO
ADDRESS: 2816 San Simeon Way
San Carlos, CA 94070-3611
FEDERAL TAX ID NUMBER/U.B.I. NUMBER: 01-0677102
TELEPHONE/EMAIL: (650) 593-9829 / davidsockol@emagined.com
COUNTY DEPT: Information Technology
DEPARTMENT CONTACT PERSON: Viggo Forde, Director
TELEPHONE/EMAIL: (425) 388-3739 / viggo.forde@snoco.org
PROJECT: Penetration Test
AMOUNT: \$66,000.00
FUND SOURCE: 505-5148614101
CONTRACT DURATION: Three (3) years from execution of the Agreement then automatically renews unless terminated in accordance with section 2.

AGREEMENT FOR PROFESSIONAL SERVICES

THIS AGREEMENT (the "Agreement") is made by and between SNOHOMISH COUNTY, a political subdivision of the State of Washington (the "County") and Emagined Security, Inc., a corporation registered to do business in the State of Washington (the "Contractor"). In consideration of the mutual benefits and covenants contained herein, the parties agree as follows:

1. Purpose of Agreement; Scope of Services. The purpose of this Agreement is for the Contractor to perform network penetration testing services for the County IT Department. The scope of services is as defined in Schedule A attached hereto and by this reference made a part hereof.

The services shall be performed in accordance with the requirements of this Agreement and with generally accepted practices prevailing in the western Washington region in the occupation or industry in which the Contractor practices or operates at the time the services are

performed. The Contractor shall perform the work in a timely manner and in accordance with the terms of this Agreement. Any materials or equipment used by the Contractor in connection with performing the services shall be of good quality. The Contractor represents that it is fully qualified to perform the services to be performed under this Agreement in a competent and professional manner.

The Contractor will prepare and present status reports and other information regarding performance of the Agreement as the County may request.

2. Term of Agreement; Time of Performance. The initial term of this Agreement shall commence upon execution (the "Effective Date") and continue for three (3) years after the Effective Date, PROVIDED, HOWEVER, that the County's obligations after December 31, 2024 are contingent upon local legislative appropriation of necessary funds for this specific purpose in accordance with the County Charter and applicable law. After the initial term, this Agreement shall renew automatically in one (1) year terms ("Renewal Term"), unless the County informs the Contractor in writing a minimum of thirty (30) days prior to the end of the then current term ("Contract Anniversary Date").

3. Compensation.

a. Services. The County will pay the Contractor for services and other direct costs as and when set forth in Schedule A, which is attached hereto and by this reference made a part of this Agreement.

b. Invoices. Upon execution of this Agreement and annually thereafter, the Contractor shall submit to the County a properly executed invoice for the flat annual fee due from the County. Subject to Section 8 of this Agreement, the County shall pay the invoice within thirty (30) calendar days of receipt.

c. Payment. The County's preferred method of payment under this contract is electronic using the County's "e-Payable" system with Bank of America. The Contractor is highly encouraged to take advantage of the electronic payment method.

In order to utilize the electronic payment method, the Contractor shall email SnocoEpayables@snoco.org and indicate it was awarded a contract with Snohomish County and will be receiving payment through the County's e-Payable process. The Contractor needs to provide contact information (name, phone number and email address). The Contractor will be contacted by a person in the Finance Accounts Payable group and assisted with the enrollment process. This should be done as soon as feasible after County award of a contract or purchase order, but not exceeding ten (10) business days.

Department approved invoices received in Finance will be processed for payment within seven calendar days for e-Payable contractors. Invoices are processed for payment by Finance two times a week for contractors who have selected the e-Payable payment option.

In the alternative, if the Contractor does not enroll in the electronic (“e-Payable”) payment method described above, contract payments will be processed by Finance with the issuance of paper checks or, if available, an alternative electronic method. Alternative payment methods, other than e-Payables, will be processed not more than 30 days from receipt of department approved invoices to Finance.

THE COUNTY MAY MAKE PAYMENTS FOR PURCHASES UNDER THIS CONTRACT USING THE COUNTY’S VISA PURCHASING CARD (PCARD).

Upon acceptance of payment, the Contractor waives any claims for the goods or services covered by the Invoice. No advance payment shall be made for the goods or services furnished by Contractor pursuant to this Contract.

d. Payment Method. In addition to Payment section above, the County may make payments for purchases under this contract using the County’s VISA purchasing card (PCARD).

Are you willing to accept PCARD payments without any fees or surcharges?

Yes No

e. Contract Maximum. Total charges under this Agreement, all fees and expenses included, shall not exceed \$66,000.00 for the Initial Term of this Agreement (excluding extensions or renewals, if any).

4. Independent Contractor. The Contractor agrees that Contractor will perform the services under this Agreement as an independent contractor and not as an agent, employee, or servant of the County. This Agreement neither constitutes nor creates an employer-employee relationship. The parties agree that the Contractor is not entitled to any benefits or rights enjoyed by employees of the County. The Contractor specifically has the right to direct and control Contractor’s own activities in providing the agreed services in accordance with the specifications set out in this Agreement. The County shall only have the right to ensure performance. Nothing in this Agreement shall be construed to render the parties partners or joint venturers.

The Contractor shall furnish, employ and have exclusive control of all persons to be engaged in performing the Contractor’s obligations under this Agreement (the “Contractor personnel”), and shall prescribe and control the means and methods of performing such obligations by providing adequate and proper supervision. Such Contractor personnel shall for all purposes be solely the employees or agents of the Contractor and shall not be deemed to be employees or agents of the County for any purposes whatsoever. With respect to Contractor personnel, the Contractor shall be solely responsible for compliance with all rules, laws and regulations relating to employment of labor, hours of labor, working conditions, payment of wages and payment of taxes, including applicable contributions from Contractor personnel when required by law.

Because it is an independent contractor, the Contractor shall be responsible for all obligations relating to federal income tax, self-employment or FICA taxes and contributions, and all other so-called employer taxes and contributions including, but not limited to, industrial insurance (workers’ compensation). The Contractor agrees to indemnify, defend and hold the

County harmless from any and all claims, valid or otherwise, made to the County because of these obligations.

The Contractor assumes full responsibility for the payment of all payroll taxes, use, sales, income, or other form of taxes, fees, licenses, excises or payments required by any city, county, federal or state legislation which are now or may during the term of the Agreement be enacted as to all persons employed by the Contractor and as to all duties, activities and requirements by the Contractor in performance of the work under this Agreement. The Contractor shall assume exclusive liability therefor, and shall meet all requirements thereunder pursuant to any rules or regulations that are now or may be promulgated in connection therewith.

5. Ownership. Upon payment of fees, any and all data, reports, analyses, documents, photographs, pamphlets, plans, specifications, surveys, films or any other materials created, prepared, produced, constructed, assembled, made, performed or otherwise produced by the Contractor or the Contractor's subcontractors or consultants for delivery to the County under this Agreement shall be the sole and absolute property of the County. Such property shall constitute "work made for hire" as defined by the U.S. Copyright Act of 1976, 17 U.S.C. § 101, and the ownership of the copyright and any other intellectual property rights in such property shall vest in the County at the time of its creation. Ownership of the intellectual property includes the right to copyright, patent, and register, and the ability to transfer these rights. Material which the Contractor uses to perform this Agreement but is not created, prepared, constructed, assembled, made, performed or otherwise produced for or paid for by the County is owned by the Contractor and is not "work made for hire" within the terms of this Agreement.

6. Changes. No changes or additions shall be made in this Agreement except as agreed to by both parties, reduced to writing and executed with the same formalities as are required for the execution of this Agreement.

7. County Contact Person. The assigned contact person (or project manager) for the County for this Agreement shall be:

Name: Fred Hartmann
Title: Division Manager of Infrastructure and Security
Department: Information Technology
Telephone: (425) 388-3998
Email: fred.hartmann@snoco.org

8. County Review and Approval. When the Contractor has completed any discrete portion of the services, the Contractor shall verify that the work is free from errors and defects and otherwise conforms to the requirements of this Agreement. The Contractor shall then notify the County that said work is complete. The County shall promptly review and inspect the work to determine whether the work is acceptable. If the County determines the work conforms to the requirements of this Agreement, the County shall notify the Contractor that the County accepts the work. If the County determines the work contains errors, omissions, or otherwise fails to conform

to the requirements of this Agreement, the County shall reject the work by providing the Contractor with written notice describing the problems with the work and describing the necessary corrections or modifications to same. In such event, the Contractor shall promptly remedy the problem or problems and re-submit the work to the County. The Contractor shall receive no additional compensation for time spent correcting errors. Payment for the work will not be made until the work is accepted by the County. The Contractor shall be responsible for the accuracy of work even after the County accepts the work.

If the Contractor fails or refuses to correct the Contractor's work when so directed by the County, the County may withhold from any payment otherwise due to the Contractor an amount that the County in good faith believes is equal to the cost the County would incur in correcting the errors, in re-procuring the work from an alternate source, and in remedying any damage caused by the Contractor's conduct.

9. Subcontracting and Assignment. The Contractor shall not subcontract, assign, or delegate any of the rights, duties or obligations covered by this Agreement without prior express written consent of the County. Any attempt by the Contractor to subcontract, assign, or delegate any portion of the Contractor's obligations under this Agreement to another party in violation of the preceding sentence shall be null and void and shall constitute a material breach of this Agreement.

10. Records and Access; Audit; Ineligible Expenditures. The Contractor shall maintain adequate records to support billings. Said records shall be maintained for a period of seven (7) years after completion of this Agreement by the Contractor. The County or any of its duly authorized representatives shall have access at reasonable times to any books, documents, papers and records of the Contractor which are directly related to this Agreement for the purposes of making audit examinations, obtaining excerpts, transcripts or copies, and ensuring compliance by the County with applicable laws. Expenditures under this Agreement, which are determined by audit to be ineligible for reimbursement and for which payment has been made to the Contractor, shall be refunded to the County by the Contractor.

11. Warranty, Limitation of Liability, Indemnity. Contractor shall perform the services provided under this Agreement with the degree of skill and care that is in accordance with then current, generally accepted professional practice and procedures.

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, CONTRACTOR SPECIFICALLY DISCLAIMS, AND COUNTY HEREBY WAIVES, ANY AND ALL PROMISES, REPRESENTATIONS AND WARRANTIES WITH RESPECT TO THE SERVICES AND PRODUCTS PROVIDED HEREUNDER, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY AS TO ITS MERCHANTABILITY, QUALITY, OPERATION OR ITS FITNESS FOR ANY PARTICULAR PURPOSE, AS WELL AS ANY WARRANTIES ALLEGED TO HAVE ARISEN FROM CUSTOM, USAGE, OR PAST DEALINGS BETWEEN THE PARTIES.

COUNTY ACKNOWLEDGES AND AGREES THAT IN NO EVENT SHALL CONTRACTOR BE LIABLE TO COUNTY, WHETHER IN CONTRACT, TORT OR OTHERWISE, FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, INDIRECT OR ECONOMIC DAMAGES, HOWEVER ARISING, AND OF WHATSOEVER NATURE, INCLUDING DAMAGES FOR LOSS OF PROFITS, LOSS OF BUSINESS, BUSINESS EXPENSE, MACHINE DOWN TIME, LOSS OF DATA, OR ANY OTHER SPECIAL OR EXEMPLARY DAMAGES, EVEN IF CONTRACTOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

NOTWITHSTANDING ANY OTHER PROVISIONS OF THIS AGREEMENT TO THE CONTRARY, THE COUNTY HEREBY ACKNOWLEDGES AND AGREES THAT CONTRACTOR'S TOTAL LIABILITY TO COUNTY SHALL IN NO CIRCUMSTANCE EXCEED THE AGGREGATE AMOUNT PAID TO CONTRACTOR PURSUANT TO THE APPLICABLE STATEMENT OF WORK OF THIS AGREEMENT FOR THE SERVICES AND PRODUCTS TO WHICH THE CLAIM RELATES.

IN NO EVENT SHALL THE TOTAL AMOUNT OF CONTRACTOR'S LIABILITY FOR ALL CLAIMS EXCEED THE AGGREGATE AMOUNT PAID TO CONTRACTOR PURSUANT TO THIS AGREEMENT.

THIS IS THE EXCLUSIVE WARRANTY, AND IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATIONS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR USE.

If required, Contractor will follow County direction regarding state / government / legal requirements and laws in capturing threat information and evidence. If the County defines additional requirements, County will be responsible for costs associated with complying with state / government / legal requirements and laws.

In the event that project services / project results performed by Contractor become of interest in third-party lawsuits (e.g., DoD False Claims Act) due to no fault of Contractor, Contractor will bill County for required Contractor time, services, or expenses (gathering evidence, attending meetings / depositions, providing witness testimony, and/or providing other legal support) in addition to legal fees accrued by Contractor.

Contractor will, at its own expense, indemnify, defend and hold harmless County and its affiliates and their respective officers, directors, employees and agents from and against any and all damages, costs, liabilities and other losses (including reasonable attorneys' fees) resulting from any third party claim arising from, or any allegation by any third party of an event or circumstance that would constitute, any breach by Contractor of any representation or warranty set forth in this Agreement, or any negligence, recklessness or willful misconduct of Contractor.

County will, at its own expense, indemnify, defend and hold harmless Contractor and its affiliates and their respective officers, directors, employees and agents from and against any and all damages, costs, liabilities and other losses (including reasonable attorneys' fees) resulting from any third party claim arising from, or any allegation by any third party of an event or circumstance

that would constitute, any breach by County of any representation or warranty set forth in this Agreement, or any negligence, recklessness or willful misconduct of County.

12. Insurance Requirements. The Contractor shall procure by the time of execution of this Agreement, and maintain for the duration of this Agreement, (i) insurance against claims for injuries to persons or damage to property which may arise from or in connection with the performance of the services hereunder by the Contractor, its agents, representatives, or employees, and (ii) a current certificate of insurance and additional insured endorsement when applicable.

a. General. Each insurance policy shall be written on an "occurrence" form, except that Professional Liability, Errors and Omissions coverage, if applicable, may be written on a claims made basis. If coverage is approved and purchased on a "claims made" basis, the Contractor warrants continuation of coverage, either through policy renewals or the purchase of an extended discovery period, if such extended coverage is available, for not less than three (3) years from the date of completion of the work which is the subject of this Agreement.

By requiring the minimum insurance coverage set forth in this Section 12, the County shall not be deemed or construed to have assessed the risks that may be applicable to the Contractor under this Agreement. The Contractor shall assess its own risks and, if it deems appropriate and/or prudent, maintain greater limits and/or broader coverage.

b. Minimum Scope and Limits of Insurance. The Contractor shall maintain coverage at least as broad as, and with limits no less than:

(i) General Liability: \$1,000,000 combined single limit per occurrence for bodily injury, personal injury and property damage, and for those policies with aggregate limits, a \$2,000,000 aggregate limit. CG 00 01 current edition, including Products and Completed Operations;

(ii) Automobile Liability: \$1,000,000 combined single limit per accident for bodily injury and property damage. CA 0001 current edition, Symbol 1;

(iii) Workers' Compensation: To meet applicable statutory requirements for workers' compensation coverage of the state or states of residency of the workers providing services under this Agreement;

(iv) Employers' Liability or "Stop Gap" coverage: \$1,000,000;

(v) Technology Professional Liability Errors & Omissions Insurance: Coverage appropriate to the Contractor's profession and work hereunder, with limits not less than \$2,000,000 per occurrence. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by the 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;

(vi) Cyber Liability Insurance: Coverage with limits not less than \$2,000,000 per occurrence or claim, \$2,000,000 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.

c. Other Insurance Provisions and Requirements. The insurance coverages required in this Agreement for all liability policies except workers' compensation and Professional Liability, if applicable, must contain, or must be endorsed to contain, the following provisions:

(i) The County, its officers, officials, employees and agents are to be covered as additional insureds as respects liability arising out of activities performed by or on behalf of the Contractor in connection with this Agreement. Such coverage shall be primary and non-contributory insurance as respects the County, its officers, officials, employees and agents. Additional Insured Endorsement shall be included with the certificate of insurance, "CG 2026 07/04" or its equivalent is required.

(ii) The Contractor's insurance coverage shall apply separately to each insured against whom a claim is made and/or lawsuit is brought, except with respect to the limits of the insurer's liability.

(iii) Any deductibles or self-insured retentions must be declared to, and approved by, the County. The deductible and/or self-insured retention of the policies shall not limit or apply to the Contractor's liability to the County and shall be the sole responsibility of the Contractor.

(iv) Insurance coverage must be placed with insurers with a Best's Underwriting Guide rating of no less than A:VIII, or, if not rated in the Best's Underwriting Guide, with minimum surpluses the equivalent of Best's surplus size VIII. Professional Liability, Errors and Omissions insurance coverage, if applicable, may be placed with insurers with a Best's rating of B+:VII. Any exception must be approved by the County.

Coverage shall not be suspended, voided, canceled, reduced in coverage or in limits until after forty-five (45) calendar days' prior written notice has been given to the County.

If at any time any of the foregoing policies fail to meet minimum requirements, the Contractor shall, upon notice to that effect from the County, promptly obtain a new policy, and shall submit the same to the County, with the appropriate certificates and endorsements, for approval.

d. Subcontractors. The Contractor shall include all subcontractors as insureds under its policies, or shall furnish separate certificates of insurance and policy endorsements for each subcontractor. **Insurance coverages provided by subcontractors instead of the Contractor as evidence of compliance with the insurance requirements of this Agreement shall be subject to all of the requirements stated herein.**

13. County Non-discrimination. It is the policy of the County to reject discrimination which denies equal treatment to any individual because of his or her race, creed, color, national origin, families with children, sex, marital status, sexual orientation, age, honorably discharged veteran or military status, or the presence of any sensory, mental, or physical disability or the use of a trained dog guide or service animal by a person with a disability as provided in Washington's Law against Discrimination, Chapter 49.60 RCW, and the Snohomish County Human Rights Ordinance, Chapter 2.460 SCC. These laws protect against specific forms of discrimination in employment, credit transactions, public accommodation, housing, county facilities and services, and county contracts.

The Contractor shall comply with the substantive requirements of Chapter 2.460 SCC, which are incorporated herein by this reference. Execution of this Agreement constitutes a certification by the Contractor of the Contractor's compliance with the requirements of Chapter 2.460 SCC. If the Contractor is found to have violated this provision, or to have furnished false or misleading information in an investigation or proceeding conducted pursuant to this Agreement or Chapter 2.460 SCC, this Agreement may be subject to a declaration of default and termination at the County's discretion. This provision shall not affect the Contractor's obligations under other federal, state, or local laws against discrimination.

14. Federal Non-discrimination. Snohomish County assures that no persons shall on the grounds of race, color, national origin, or sex as provided by Title VI of the Civil Rights Act of 1964 (Pub. L. No. 88-352), as amended, and the Civil Rights Restoration Act of 1987 (Pub. L. No. 100-259) be excluded from participation in, be denied the benefits of, or be otherwise subjected to discrimination under any County sponsored program or activity. Snohomish County further assures that every effort will be made to ensure nondiscrimination in all of its programs and activities, whether those programs and activities are federally funded or not.

15. Employment of County Employees. SCC 2.50.075, "Restrictions on future employment of County employees," imposes certain restrictions on the subsequent employment and compensation of County employees. The Contractor represents and warrants to the County that it does not at the time of execution of this Agreement, and that it shall not during the term of this Agreement, employ a former or current County employee in violation of SCC 2.50.075. For breach or violation of these representations and warranties, the County shall have the right to terminate this Agreement without liability.

16. Compliance with Other Laws. The Contractor shall comply with all other applicable federal, state and local laws, rules, and regulations in performing this Agreement.

17. Compliance with Grant Terms and Conditions. The Contractor shall comply with any and all conditions, terms and requirements of any federal, state or other grant, if any, that wholly or partially funds the Contractor's work hereunder.

18. Prohibition of Contingency Fee Arrangements. The Contractor warrants that it has not employed or retained any company or person, other than a bona fide employee working solely for the Contractor, to solicit or secure this Agreement and that it has not paid or agreed to pay any company or person, other than a bona fide employee working solely for the Contractor, any fee, commission, percentage, brokerage fee, gifts or any other consideration, contingent upon or resulting from the award or making of this Agreement. For breach or violation of this warranty, the County shall have the right to terminate 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, commission, percentage, brokerage fee, gift or contingent fee.

19. Force Majeure. If either party is unable to perform any of its obligations under this Agreement as a direct result of an unforeseeable event beyond that party's reasonable control, including but not limited to an act of war, act of nature (including but not limited to earthquake and flood), embargo, riot, sabotage, labor shortage or dispute (despite due diligence in obtaining the same), or governmental restriction imposed subsequent to execution of the Agreement (collectively, a "force majeure event"), the time for performance shall be extended by the number of days directly attributable to the force majeure event. Both parties agree to use their best efforts to minimize the effects of such failures or delays.

20. Suspension of Work. The County may, at any time, instruct the Contractor in writing to stop work effective immediately, or as directed, pending either further instructions from the County to resume the work or a notice from the County of breach or termination under Section 21 of this Agreement.

21. Non-Waiver of Breach; Termination.

a. The failure of the County to insist upon strict performance of any of the covenants or agreements contained in this Agreement, or to exercise any option conferred by this Agreement, in one or more instances shall not be construed to be a waiver or relinquishment of those covenants, agreements or options, and the same shall be and remain in full force and effect.

b. If the Contractor breaches any of its obligations hereunder, and fails to cure the same within five (5) business days of written notice to do so by the County, the County may terminate this Agreement, in which case the County shall pay the Contractor only for the services and corresponding reimbursable expenses, if any, accepted by the County in accordance with Sections 3 and 8 hereof.

c. The County may terminate this Agreement upon two (2) business days' written notice to the Contractor for any reason other than stated in subparagraph b above, in which case payment shall be made in accordance with Sections 3 and 8 hereof for the services and

corresponding reimbursable expenses, if any, reasonably and directly incurred by the Contractor in performing this Agreement prior to receipt of the termination notice.

d. Termination by the County hereunder shall not affect the rights of the County as against the Contractor provided under any other section or paragraph herein. The County does not, by exercising its rights under this Section 21, waive, release or forego any legal remedy for any violation, breach or non-performance of any of the provisions of this Agreement. At its sole option, the County may deduct from the final payment due the Contractor (i) any damages, expenses or costs arising out of any such violations, breaches or non-performance and (ii) any other set-offs or credits including, but not limited to, the costs to the County of selecting and compensating another contractor to complete the work of the Agreement.

22. Notices. All notices and other communications shall be in writing and shall be sufficient if given, and shall be deemed given, on the date on which the same has been mailed by certified mail, return receipt requested, postage prepaid, addressed as follows:

If to the County: Snohomish County Information Technology
3000 Rockefeller Ave., M/S 709
Everett, Washington 98201
Attention: Dee White
Senior IT Contract Specialist

and to: Snohomish County Purchasing Division
3000 Rockefeller Avenue, M/S 507
Everett, Washington 98201
Attention: Purchasing Manager

If to the Contractor: Emagined Security, Inc.
2816 San Simeon Way
San Carlos, CA 94070-3611
Attention: David Sockol
CEO

The County or the Contractor may, by notice to the other given hereunder, designate any further or different addresses to which subsequent notices or other communications shall be sent.

23. Confidentiality. The Contractor shall not disclose, transfer, sell or otherwise release to any third party any Confidential Information as defined in Schedule B gained by reason of or otherwise in connection with the Contractor's performance under this Agreement. The Contractor may use such information solely for the purposes necessary to perform its obligations under this Agreement. The Contractor shall promptly give written notice to the County of any judicial proceeding seeking disclosure of such information.

24. Public Records Act. This Agreement and all public records associated with this

Agreement shall be available from the County for inspection and copying by the public where required by the Public Records Act, Chapter 42.56 RCW (the "Act"). To the extent that public records then in the custody of the Contractor are needed for the County to respond to a request under the Act, as determined by the County, the Contractor agrees to make them promptly available to the County. If the Contractor considers any portion of any record provided to the County under this Agreement, whether in electronic or hard copy form, to be protected from disclosure under law, the Contractor shall clearly identify any specific information that it claims to be confidential or proprietary. If the County receives a request under the Act to inspect or copy the information so identified by the Contractor and the County determines that release of the information is required by the Act or otherwise appropriate, the County's sole obligations shall be to notify the Contractor (a) of the request and (b) of the date that such information will be released to the requester unless the Contractor obtains a court order to enjoin that disclosure pursuant to RCW 42.56.540. If the Contractor fails to timely obtain a court order enjoining disclosure, the County will release the requested information on the date specified.

The County has, and by this section assumes, no obligation on behalf of the Contractor to claim any exemption from disclosure under the Act. The County shall not be liable to the Contractor for releasing records not clearly identified by the Contractor as confidential or proprietary. The County shall not be liable to the Contractor for any records that the County releases in compliance with this section or in compliance with an order of a court of competent jurisdiction.

25. Interpretation. This Agreement and each of the terms and provisions of it are deemed to have been explicitly negotiated by the parties. The language in all parts of this Agreement shall, in all cases, be construed according to its fair meaning and not strictly for or against either of the parties hereto. The captions and headings of this Agreement are used only for convenience and are not intended to affect the interpretation of the provisions of this Agreement. This Agreement shall be construed so that wherever applicable the use of the singular number shall include the plural number, and vice versa, and the use of any gender shall be applicable to all genders.

26. Complete Agreement. This Agreement, including Schedule A Statement of Work, and Schedule B Mutual Non-Disclosure Agreement, constitutes the entire understanding of the parties. Any written or verbal agreements that are not set forth herein or incorporated herein by reference are expressly excluded.

27. Conflicts between Attachments and Text. Should any conflicts exist between any attached exhibit or schedule and the text or main body of this Agreement, the text or main body of this Agreement shall prevail.

28. No Third Party Beneficiaries. The provisions of this Agreement are for the exclusive benefit of the County and the Contractor. This Agreement shall not be deemed to have conferred any rights, express or implied, upon any third parties.

29. Governing Law; Venue. This Agreement shall be governed by the laws of the State of Washington. The venue of any action arising out of this Agreement shall be in the Superior Court of the State of Washington, in and for Snohomish County.

30. Severability. Should any clause, phrase, sentence or paragraph of this agreement be declared invalid or void, the remaining provisions of this Agreement shall remain in full force and effect.

31. Authority. Each signatory to this Agreement represents that he or she has full and sufficient authority to execute this Agreement on behalf of the County or the Contractor, as the case may be, and that upon execution of this Agreement it shall constitute a binding obligation of the County or the Contractor, as the case may be.

32. Survival. Those provisions of this Agreement that by their sense and purpose should survive expiration or termination of the Agreement shall so survive.

33. Execution in Counterparts. This Agreement may be executed in counterparts, each of which shall constitute an original and all of which shall constitute one and the same Agreement.

SNOHOMISH COUNTY:

EMAGINED SECURITY, INC.

County Executive Ken Klein Date
Executive Director

 Jan 10, 2024

Title Date

Approved as to insurance
and indemnification provisions:

Approved as to form only:

Barker, Sheila Digitally signed by Barker, Sheila
Date: 2024.01.11 08:21:24 -08'00'

Risk Management Date

Legal Counsel to the Contractor Date

COUNCIL USE ONLY	
Approved	<u>1/24/2024</u>
ECAF #	<u>2024-0005</u>
MOT/ORD	<u>Motion 24-018</u>

Schedule A Statement of Work: External and Internal Penetration Test

For: Snohomish County



Phone: (650) 593-9829
Mail: info@emagined.com
Web: www.emagined.com

Copyright © 2023 All rights reserved

This SOW is a copyright of Emagined Security and is not to be forwarded in whole or in part to third parties without the written consent of Emagined Security.

STATEMENT OF WORK

This Statement of Work (SOW) is an agreement by and between EMAGINED SECURITY, INC. (EMAGINED) and SNOHOMISH COUNTY (CUSTOMER).

Statement of Work Title: External and Internal Penetration Test

1. Description of Work:

Penetration Test Service Overview

EMAGINED defines its penetration testing services as the following levels:

Escalating Level

- **Level 4 – Escalating Penetration Test:** This version includes all tasks performed in the Expanded Penetration Test (Level 3) and adds in attack aggressiveness and sophistication over time with each subsequent test. Escalating Penetration Testing includes:
 - One (1) penetration test to establish a CUSTOMER baseline
 - Three (3) follow-on penetration tests within the same 12-month contiguous period which increases in attack aggressiveness and sophistication over time, and with each subsequent test iteration

These tests are designed to demonstrate what a trained and dedicated attacker might accomplish over an extended period. Additionally, Emagined shall enhance the test to include upon CUSTOMER request, the following:

- Industry Monitoring
- Dedicated research of CUSTOMER specific, potential or requested vulnerabilities
- Validation of newly discovered attack vectors
- Application of industry currently emerging threats
- Attack Recidivism

Standard Testing Levels

- **Level 3 – Expanded Penetration Test:** This version includes all tasks performed in the Penetration Test (Level 2) and adds advanced exploitation, persistence and pivoting. Additionally, Expanded Penetration Testing can be used to:
 - Focus on identifying zero-day vulnerabilities – industry notification to be fully discussed with CUSTOMER to ensure appropriate / timely disclosure
 - Validate the effectiveness of existing security controls or awareness efforts
 - Evaluate intrusion detection effectiveness
 - Test incident response capabilities

This testing level is designed to demonstrate what a trained and dedicated attacker might reasonably accomplish during the testing period. This is the most extensive version of point in time test.

- **Level 2 – Penetration Test:** This version includes all tasks performed in the Vulnerability Assessment (Level 1) and adds vulnerability exploitation within the defined scope. This is the default (i.e., recommended) version of the test. Testing includes:
 - EMAGINED testing is designed to be exhaustive, which means that EMAGINED will not stop at the first successful penetration but will continue to identify additional vulnerabilities and attack vectors
 - EMAGINED uses a combination of automated and custom-built testing tools to identify both known vulnerabilities (those that are found in the CVE database) as well as identifying unknown vulnerabilities that cannot be identified using only automated tools
 - Basic Level Remediation Validation available at no charge within 30 days on same network / application code base
 - A single validation of up to 5 basic level findings (e.g., OWASP Top 10) identified in the initial report to check if they have been remediated
 - CREST certified testing uplift available at Level 2 (follows CREST approved testing methodology, CREST logo on reports, satisfies EU testing requirements)



Other Testing Levels (Typically Not Available as a Stand-Alone Service)

- **Level 1 – Vulnerability Assessment:** This version includes automated and manual scans and manual validation of vulnerabilities. Some assessment and analysis may be performed. This is the minimal version of the test.

- **Level 0 – Vulnerability Scan:** This version includes a basic automated scan to satisfy regulatory requirements utilizing a single vulnerability tool. The associated deliverable is limited to only raw (i.e. canned) reports from the tool. No analysis or manual validation of results is performed.

For the purpose of this document, unless specified as a different level, the **Level 2 - Penetration Test** will be performed by EMAGINED personnel. EMAGINED personnel are United States of America citizens (services are not outsourced) and have required background checks.

Unless other arrangements are agreed upon, per the optional CUSTOMER Equipment Build, EMAGINED will use EMAGINED hardware and software connected to the CUSTOMER network to perform testing.

TASK 1: External Network Penetration Test

EMAGINED will perform an external penetration test against the Internet architecture (i.e., firewalls, DNS servers, routers, switches, load balancers, and supporting systems).

As such, EMAGINED will attempt to identify the implemented security controls or lack of controls protecting against Internet-based attacks. Access attempts to the servers to scan for vulnerabilities will take place from a location on the Internet, to mimic standard access rights available to general Internet users.

If EMAGINED successfully penetrates the firewall and/or other filtering devices, EMAGINED will attempt to gain access to systems behind the security mechanism. By attempting to gain access to the systems on the subnet, EMAGINED will attempt to identify risks associated with the current security configuration. Testing will be **limited to 70 Total Active IPs**.

The Penetration Test will begin with passive probes that are designed to avoid detection and will be escalated to aggressive active tests that should be easily detected. The penetration test of the Internet-facing architecture will be structured as follows:

Passive Data Collection:

The initial phase of any security review involves extensive data collection and penetration studies are no exception. The following methods may be used as part of this information-gathering phase:

- Web searches and newsgroup browsing
- DNS zone transfers, InterNIC type queries
- IP scanning and SNMP sweeps
- Network mapping with traceroute and other tools
- Social Engineering (if allowed)
- Initial target identification

Active Intrusion:

Once the active intrusion phase is begun, targets are more likely to be alerted to suspicious activity. This phase serves to identify potential or known vulnerabilities that could be exploited by intruders. This is the main analysis phase that correlates the information gathered. Methods for performing this phase can include:

- Vulnerability scanning
- Port scanning

Aggressive Penetration:

The aggressive phase is typically only used when a CUSTOMER needs to demonstrate actual data or system compromises. This phase involves utilizing the identified vulnerabilities to gain access to internal systems and networks. This phase typically utilizes many tools that may be available in the public domain and are used by actual intruders. The penetration agreement tightly controls the methods used during this phase, and activities are logged extensively.

TASK 2: Internal Network Penetration Test

EMAGINED will perform an internal penetration test against the CUSTOMER's internal network. As such, EMAGINED will attempt to identify the implemented security controls or lack of controls protecting against internal-based attacks to sensitive areas. Access attempts to the servers to scan for vulnerabilities will take place from a location on the internal network, to mimic standard access rights available to general internal users.

EMAGINED will investigate potential vulnerabilities while posing as an individual with only physical access to the network and/or as an authorized user with normal access rights. If a test is requested to be performed as an authorized user, EMAGINED will require normal user access to the network on the appropriate segment.

EMAGINED will assess the internal controls between the targeted sensitive network segment and the connection segment. If access to the targeted network segment is achieved, EMAGINED will attempt to gain access to at least one system that attached to the network segment.

EMAGINED will perform penetration testing from the Remote EMAGINED office(s) only via remote connectivity to a Kali ISO installation (Sensor). EMAGINED recommends that CUSTOMER contract for a sensor in each discrete location. If CUSTOMER chooses to scan from one sensor to multiple remote locations, CUSTOMER is responsible for connection stability and must notify EMAGINED if high utilization is experienced. If additional virtual sensors are required after test initiation, optional service fees may be required. Testing will be performed from the following sensor locations:

Sensor Location 1:

Up to **400 active IP addresses** (sample set test size)

No penetration testing will be performed from the other locations.

The Penetration Test will begin with passive probes that are designed to avoid detection and will be escalated to aggressive active tests that should be easily detected. The penetration assessment will be structured as follows:

Passive Data Collection:

The initial phase involves extensive data collection to identify system information or access parameters.

Active Intrusion:

This phase serves to identify potential or known vulnerabilities that could be exploited by intruders. This is the main analysis phase that correlates the information gathered.

Aggressive Penetration:

This phase involves actually utilizing identified vulnerabilities to gain access to internal systems and networks. This phase typically utilizes many tools that may be available in the public domain and are used by actual intruders. The methods used during this phase are tightly controlled by the penetration agreement and activities are extensively logged.

TASK 3: Penetration Test Deliverable Creation

For Penetration Test tasks, EMAGINED will prepare a report of our findings for CUSTOMER within 2 weeks of completing the assessment in EMAGINED format unless otherwise agreed before reporting has commenced. The report will be delivered first in draft form to allow time for the CUSTOMER to prepare a response. Upon receipt of the response from the CUSTOMER, EMAGINED will prepare a final report, which will incorporate CUSTOMER responses. After 5 days draft deliverables will become final. Any changes to the deliverable after the 5-day review period will be performed on a Time & Materials basis.

This report will contain at least the following information, which will address the concerns discovered during the review:

- **Executive Summary:** This part of the report will address the overall security posture of the environment reviewed and highlight the major findings.
- **Engagement Objective:** The section will include the objectives and a description of the tasks performed by EMAGINED.
- **Testing Methodology:** A high-level description of EMAGINED's methodology used for performing the assessment will be documented in this area.
- **Identified Vulnerabilities and Severities:** A separate section will be devoted to the findings discovered during the engagement. Each finding will provide detailed information as to the issue of concern and possible remediation or resolution to the problem. This section will, as appropriate, have a technical focus.
- **Conclusions:** This area details EMAGINED's overall recommendations based on the findings during the assessment.

Each identified finding will be labeled with a severity rating, as follows:

- **Critical:** Findings at this level may be used to immediately breach the integrity of the environment and/or organization. This level of severity should be addressed immediately. In addition to addressing the issue, action should be taken to ensure a compromise has not already taken place. Findings in this severity classification should be worked until closed.
- **High:** Findings at this level are serious deficiencies that have already, can, or most likely, will result in serious breaches in the hosting infrastructure's ability to maintain its security posture. The system, application or data that would be compromised is considered critical to the operation of the organization. Findings in this severity classification should be remediated immediately.
- **Medium:** Findings at this level of severity could have a moderate impact on the organization if an attack were successful. The system, application or data that would be compromised are considered sensitive and should not be in the public domain but are not considered mission-critical or the Client's proprietary/trade secret. Findings in this severity should be remediated at the next earliest opportunity but are not as urgent a priority as those in higher severity classifications.
- **Low:** Findings at this level of severity allow an attacker to gain knowledge of the organization. They do not constitute a direct threat to the organization individually but are the building blocks that attackers use to string together a successful assault on the organization. Findings in this severity should be remediated at the next earliest maintenance window or scheduled service period.
- **Informational:** Findings at this level of severity do not directly affect the security posture of the organization. Issues slant toward informational, often with a disclosure-based output, and may aid an attacker with reconnaissance, enumeration or deduction of viable assets and underlying technologies that could assist with vulnerability identification. Findings in this severity should be considered for remediation at the earliest convenience.

Additionally, each finding identified has been categorized as to the difficulty of exploitation. The difficulty of exploitation is subdivided into the following categories:

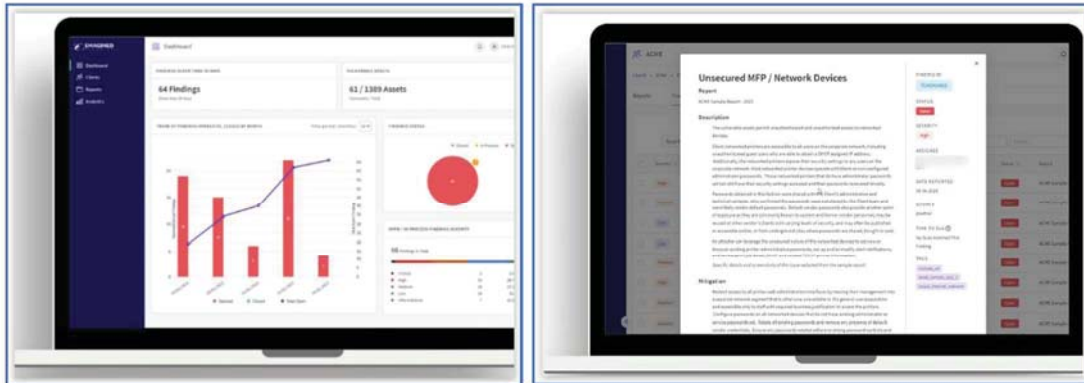
- **Easy:** A finding that can be easily exploited by commonly available tools on the internet, well-known exploits, and/or where little to no technical expertise is required.
- **Moderate:** Findings that require a medium level of efforts such as creating procedures, obscure command line parameters, and some technical expertise are required.
- **Hard:** Findings that require the use of custom developed tools and procedures, programming skills, and detailed technical expertise is required.

Within each identified vulnerability, when available, EMAGINED will provide screen shots of the identified vulnerabilities, configuration files and actual test results.

Any critical findings identified during the testing process will be communicated immediately to CUSTOMER management for appropriate action.

TASK 4: CLARITY External Vulnerability Scans (Quarterly No Charge Value-Ad Service)

As described in Attachment 1, Brochures, EMAGINED will provide (at EMAGINED’s discretion as this is a value-add service only) vulnerability scans of the same 70 external IP addresses from the prior task identified by CUSTOMER for three (3) follow-on quarters. Scans will be run by EMAGINED and results will be provided via the EMAGINED CLARITY platform (<https://www.emagined.com/clarity>).



The associated deliverable is limited to standard output from the CLARITY platform. No EMAGINED analysis of results will be performed. Via the CLARITY platform, CUSTOMER will be able to perform findings review, collaborate on remediation, and access the results on their own in order to support a Vulnerability Management program.

2. Test Requirement Details

EMAGINED will work closely with CUSTOMER technical and management points of contact during testing:

- Points of contact will be required to coordinate and schedule mutually acceptable dates for the start of the testing
- Assigned points of contacts must be authorized to make test scope and scheduling decisions
- All communications regarding scheduling must include a time zone
- Points of contacts must respond to EMAGINED email request / confirmations in writing

EMAGINED requires the following information prior to starting testing:

- Dedicated credentials for testing only, as required
- Network diagram of Internet and Internal Infrastructure including connection speeds
- IP address of the firewalls, DNS servers, routers, switches, load balancers, and supporting systems
- Available documentation describing system process flows for application / API testing

EMAGINED requires the following network infrastructure disclosures prior to starting testing:

- End of Life / End of Service networking / routing equipment (inherently unstable)

- Any low bandwidth or wireless connections in scope
- Non-Enterprise class networking / routing equipment
- IP address of the internal systems to be excluded from scope

EMAGINED requests that our IP addresses be whitelisted from security device inspection (e.g., IDS, IPS, WAF) in order for the test(s) to be an accurate representation of a slow methodical attacker:

- If testing conducted with perimeter protection controls in place with no whitelisting, results should be considered “as is” and may not provide an accurate reflection of the security posture or vulnerabilities present in the environment / application
- Not whitelisting scanning tools on internal network test can cause an interruption in service

EMAGINED will store provided CUSTOMER data and results in a protected Microsoft SharePoint environment with Discretionary Access Controls and in EMAGINED’s Proprietary Reporting Tool which is protected by Two-Factor Authentication, Discretionary Access Controls, Encryption within a SOC II AWS protected environment. EMAGINED will encrypt communications if they contain sensitive data. EMAGINED will utilize Antivirus tools on testing systems to prevent the targets being infected with malicious software.

EMAGINED requires that CUSTOMER have a change management freeze in place during the testing windows.

3. Deliverable Acceptance / Constraints

EMAGINED will prepare a deliverable(s) addressing results for the tasks described above. The draft deliverable(s) shall be delivered to the CUSTOMER as they are created. Deliverables will be in EMAGINED Standard Formats.

The documents will be delivered in first draft form to allow time for the CUSTOMER to prepare a consolidated set of comments. CUSTOMER review duration will be two calendar weeks. After the review duration, deliverables will become final whether or not EMAGINED has received comments from CUSTOMER. Any requested changes to deliverables, after report finalization, will be performed on a Time & Materials basis.

Upon receipt of the comments from the CUSTOMER, EMAGINED will prepare the final documents, which will incorporate the responses.

4. Timeframe:

EMAGINED will work with CUSTOMER to arrive at a mutually acceptable work schedule. EMAGINED will attempt to schedule projects to begin as quickly as possible after execution of the Agreement while considering CUSTOMER Requested Dates. Projects are formally scheduled after execution of the Agreement on a first-come, first-served basis. If CUSTOMER is not available for schedule timeframe, it will be necessary for EMAGINED to reschedule project activities.

All Services will be performed during Normal Work Hours. “Normal Work Hours” means a standard, consecutive nine (9) hour workday, including a one (1) hour meal break. Hours do not include weekends,

public holidays (observed in the country where services are performed), or hours between 7 p.m. and 7 a.m. local time (EMAGINED personnel’s physical time zones).

Note: Higher levels of effort typically lead to better and more accurate results. The degree to which CUSTOMER has developed plans, strategies, and requirements and has gathered existing documentation will directly impact the work effort required.

5. Annual Auto Renewal (3 Year Minimum):

CUSTOMER agrees the contract minimum is three (3) years and then auto renews on the Contract Anniversary Date for the same scope, unless CUSTOMER informs EMAGINED at least thirty (30) days prior to the Contract Anniversary Date and CUSTOMER has removed any EMAGINED licensed tools. If the scope needs to be modified, CUSTOMER agrees to contact EMAGINED at least ninety (90) days in advance of the Contract Anniversary Date to request a change order, which may require a written amendment to the Agreement.

Beginning with the fourth year, EMAGINED further reserves the right to modify the pricing terms stated below by giving CUSTOMER at least ninety (90) days advance written notice prior to the Contract Anniversary Date.

6. Work Location

EMAGINED will work with CUSTOMER from EMAGINED location(s) during the engagement. No travel is included in this SOW. If travel is required, a change order must be authorized.

7. Fees and costs:

Fixed Price fees are calculated as follows:

Fixed Price

The fee to perform the Penetration Test is a firm-fixed-price plus other direct costs (ODC’s) as described in this Section 7 of Schedule A, if required.

Project Task	Quantity (Details)	Annual Cost
▪ External Network Penetration Test	70 IPs	\$13,000
▪ Internal Network Penetration Test	400 IPs	\$11,000
▪ Physical Remote Sensor Fee (\$500 Per)	1 Sensor	\$500
▪ Deliverable Creation	1 Report	N/C
▪ CLARITY External Vulnerability Scans (Quarterly No Charge Value-Add Service)	3 Quarters - 70 IPs	N/C – Value Add
TOTAL ANNUAL COST (USD)		\$ 24,500

<ul style="list-style-type: none"> ▪ Discount for 3 Year Commit with Auto Renewal 	3 Year Annual Discount	<\$2,500>
TOTAL ANNUAL COST AFTER DISCOUNT (USD)		\$ 22,000

Expenses / Other Direct Costs

CUSTOMER will be responsible for expenses incurred for the purchase, rent, or lease of any specialty hardware and software required by the scope of this project approved by CUSTOMER.

8. Invoicing:

EMAGINED shall invoice CUSTOMER in accordance with section 3.b. of the Agreement.

Other Direct Costs, if any, will be invoiced monthly. EMAGINED shall provide CUSTOMER supporting documentation upon request.

Late payments will accrue interest at the rate of one percent (1%) per month if payment is past the net due date.

9. Assumptions & Considerations:

EMAGINED has made the following assumptions and considerations in the development of this Statement of Work:

- CUSTOMER must meet established timelines to retain project execution dates. If CUSTOMER does not meet established timelines, it will be necessary for EMAGINED to reschedule project activities (rescheduling can cause delays of several weeks).
- **All CUSTOMER penetration testing pre-engagement criteria must be available at least one business week in advance for pre-engagement connectivity testing and to preserve testing timetable (as applicable):**
 - Remote Sensors
 - Usernames & passwords credentials (application, network, login, etc.)
 - Application URLs
 - IP Addresses
 - Remote Access (e.g., SSH) & VPN
- If CUSTOMER does not reschedule the test with missing/delayed/incorrect pre-engagement criteria (e.g., testing credentials) with less than one-week notice, the test will be subject to project delay fees while EMAGINED is waiting for issues to be resolved.
- EMAGINED will perform all work remotely.
- If CUSTOMER needs to cancel meetings, EMAGINED respectfully request at least 24 hours' notice.

- CUSTOMER will provide sufficient resources for work on-site, including office space, network connections, phone lines, etc. for the personnel who will be on-site.
- EMAGINED expects a mutually beneficial, collaborative, and healthy working environment. In the event either party experiences an environment that does not meet this requirement, management escalation is required. Steps must be taken to correct this situation up to and including resource assignment changes or project cancellation.
- In conducting the project, EMAGINED's security expert may draw on other EMAGINED's personnel to address specific issues, as required. This assigned lead, and other supporting staff, will utilize hours from the maximum assigned to the project. As individual tasks are completed, the results will be forwarded to CUSTOMER personnel.
- EMAGINED may adjust resource scheduling to accommodate other client's requests as long as the adjustment does not impact delivery dates as identified in this Statement of Work.
- Only those services listed above are to be considered in scope unless mutually agreed upon. If any additional services are required or requested, or project scope is reduced or cancelled, a change order will be required.

CUSTOMER will work with EMAGINED to help minimize expenses. This includes efforts such as grouping on-site activities during consecutive days to defray travel expenditures if any.

10. Terms & Conditions:

CUSTOMER hereby accepts the services and the related terms and conditions set forth in this Statement of Work (SOW). CUSTOMER expressly acknowledges that the performance of these services will require EMAGINED to gain access to CUSTOMER's confidential and proprietary network and information assets and authorizes this access for the purposes described in the SOW, subject, however, to Schedule B, the Mutual Nondisclosure Agreement (NDA), between CUSTOMER and EMAGINED.

SECURITY REQUIREMENTS

The County does not offer unlimited Contractor access to servers housed in the County Data Center. The County shall create a Contractor access account, as needed. Server access shall be coordinated against internal change control request and access is facilitated via Citrix. No other Contractor access application use is supported by the County.

The Contractor shall instruct its employees, agents, and subcontractors that they shall comply with the County's security, access, and safety requirements for the protection of the County's facilities and employees while on the County's premises.

CJIS. Contractor shall comply with the Criminal Justice Information Services (CJIS) Security Policy of the U.S. Federal Bureau of Investigation (FBI) and sign CJIS security agreements, including allowing or performing any required employee background checks according to the CJIS policy, and completing online CJIS training and certification. Contractor shall ensure that all staff working with the County are CJIS certified.

Due to the nature of the services contemplated by the SOW, CUSTOMER acknowledges that no representation or warranty can be made by EMAGINED with respect to such services or the efficacy thereof. In particular, CUSTOMER acknowledges that damage to CUSTOMER's systems or information could result from the performance of such services, and that, following completion of such services, there can be no assurance that CUSTOMER's network will be secure or that unauthorized access thereof will not occur. WITHOUT LIMITING THE FOREGOING, EMAGINED MAKES NO EXPRESS OR IMPLIED REPRESENTATIONS WITH RESPECT TO ITS PERFORMANCE OF THE SERVICES HEREUNDER OR ANY DELIVERABLES CONTEMPLATED HEREBY, INCLUDING WITHOUT LIMITATION ANY REPRESENTATION OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

CUSTOMER expressly authorizes EMAGINED to gain access, including without limitation external network access and without regard to CUSTOMER Information Security Policy, to CUSTOMER's computer network and information systems which is reasonable and necessary, in EMAGINED' sole judgment, for the purposes described in the SOW, and CUSTOMER acknowledges that such access shall be obtained by EMAGINED with the express permission of CUSTOMER. To CUSTOMER's knowledge, such access is not a violation of any federal, state or local laws, rules or regulations, including without limitation the Computer Crime Act of 1986, as amended, or the Economic Espionage Act of 1996, as amended, and CUSTOMER agrees not to bring any charges or claims against EMAGINED based on such activities. Execution of this SOW by the representative of CUSTOMER shall constitute a representation and warranty by CUSTOMER that such representative is duly authorized to do so and has received all requisite governmental consents and approvals which may be necessary or appropriate to execute this SOW and to carry out the terms hereof, including without limitation the preceding sentence.

If required, EMAGINED will follow CUSTOMER's counsel direction regarding state / government / legal requirements and laws in capturing threat information and evidence. If CUSTOMER's counsel defines additional requirements, CUSTOMER will be responsible for costs associated with complying with state / government / legal requirements and laws.

In the event that project services / project results performed by EMAGINED become of interest in third-party lawsuits (e.g., False Claims Act) due to no fault of EMAGINED, EMAGINED will bill (at Standard Rates) CUSTOMER for required EMAGINED time, services, or expenses (gathering evidence, attending meetings / depositions, providing witness testimony, and/or providing other legal support) in addition to legal fees accrued by EMAGINED.

11. Confidentiality / Mutual Nondisclosure Agreement (NDA)

Each party hereby acknowledges that it may be exposed to confidential and/or proprietary information of the other party, including, without limitation, custom work products, embedded software and other technical information (including functional and technical specifications, designs, drawings, analysis, research, processes, computer programs, methods, ideas, "know how" and the like), business information (sales and marketing research, materials, plans, accounting and financial information, personnel records and the like) and other information expressly designated as confidential ("Confidential Information"). Confidential Information does not include:

- information already known or independently developed by the recipient
- information in the public domain through no wrongful act on the part of the recipient

- information received by the recipient from a third party who to the best of recipient's knowledge was free to disclose it
- information disclosed pursuant to the provisions of a court order

With respect to the other party's Confidential Information, the recipient hereby agrees that during the term of this Agreement, and for a period of one year thereafter, it will not use, commercialize or disclose such Confidential Information to any person or entity, except in accordance with Chapter 42.56 RCW, or to its own employees having a "need to know" (and who are themselves bound by similar non-disclosure restrictions). Neither party nor any recipient may alter or remove from any software or associated documentation owned or provided by the other party any proprietary, copyright, trademark or trade secret legend. Each party shall use at least the same degree of care in safeguarding the other party's Confidential Information as it uses in safeguarding its own Confidential Information.

12. Intellectual Property Rights & Ownership of Final Work Products:

Upon final payment, EMAGINED hereby grants CUSTOMER and its Affiliates a nonexclusive, sublicensable, worldwide, royalty-free license to access and use any pre-existing Work Product and intellectual property integrated into any Deliverables and Work Product. EMAGINED authorizes CUSTOMER and its Affiliates to use any Work Product so long as such use is not to create derivative works and, if disclosed to a third party, is subject to a written nondisclosure agreement requiring such third party to maintain the confidentiality of such Work Product.

EMAGINED shall own all right title and interest in EMAGINED's pre-existing trade secrets, Confidential Information or other proprietary rights in any pre-existing creative or proprietary ideas, information, or other material used or enhanced by EMAGINED or presented to CUSTOMER that was developed or acquired by EMAGINED prior to or during the performance of the Services under any Exhibit governing the Deliverables or that is licensed by EMAGINED from any third party including, but not limited to: data, software, modules, components, designs, utilities, databases, subsets, objects, program listings, tools, models, methodologies, programs, systems, analysis frameworks, leading practices, report formats, manner of data expression and specifications.

To the extent that CUSTOMER provides any feedback to EMAGINED's pre-existing trade secrets, CUSTOMER grants to EMAGINED a perpetual, irrevocable, worldwide, nonexclusive, transferable, sublicensable, royalty-free, fully paid-up right and license to use and commercially utilize the feedback in any manner EMAGINED deems fit.

13. Marketing Use of Name:

CUSTOMER may provide written authorization for EMAGINED to use CUSTOMER's name and logo on EMAGINED's website and within marketing material. If CUSTOMER would like to provide testimonials / quotes for use on EMAGINED's website and within marketing material, EMAGINED will validate in writing the wording to ensure that comments are accurately portrayed.

14. Specific Project Terms & Conditions:

CUSTOMER has requested said penetration test and thus agrees to the inherent risks associated with a penetration attack. EMAGINED agrees to perform this review in a diligent and professional manner and

without malicious intent. CUSTOMER agrees not to pursue EMAGINED or the Internet Service Provider (ISP) used for unforeseen consequences (e.g., performance degradations or system unavailability) associated with the provisions in this agreement. As such, CUSTOMER agrees to accept any and all risks associated with the Services.

CUSTOMER declares that EMAGINED has the authorization to access associated computers, computer systems, and computer networks in order to perform the services detailed in this Agreement. For the purposes of EMAGINED's or its agent's performance of any penetration or intrusion testing tasks issued by CUSTOMER and agreed to by EMAGINED under this Agreement, CUSTOMER hereby authorizes EMAGINED to intercept, monitor, study and/or register any and all communications from or to CUSTOMER's computer systems necessary to carry out the scope of work under the Agreement.

CUSTOMER declares that EMAGINED has authorization to perform a dark web scan, view & test results, and report back compromised information associated with CUSTOMER's domain, IP address, email addresses, and other indicators. This information may include sensitive information such as plaintext passwords and other personally identifiable information on CUSTOMER's current and/or former employees.

CUSTOMER declares that it has obtained all required approvals needed for EMAGINED to perform the services detailed in this Agreement. CUSTOMER grants access to associated systems, networks, equipment, software, and information necessary without violating the rights of any third party. CUSTOMER agrees to indemnify and hold EMAGINED harmless for any damages or liability resulting from third party claims that EMAGINED did not have the authorization to obtain such access.

CUSTOMER understands that comprehensive penetration testing requires that adequate time be allotted to perform testing. In the event that EMAGINED is required to reduce testing time to meet CUSTOMER deadlines, EMAGINED will place a disclaimer on the report similar to the following as appropriate "Due to scheduling constraints beyond EMAGINED's control, testing was limited in the number of viable testing hours available within the scheduled engagement window. As such, the CUSTOMER should bear in mind that the results presented herein may not be as representative nor as comprehensive of the target environment's vulnerability and attack surface as might have been identified during the initially scheduled, time-boxed testing window. Results should be viewed accordingly, and further testing considered when more conducive with to the CUSTOMER's schedule."

CUSTOMER understands that the penetration test to be performed as a result of this Agreement is an uncertain process. In this regard, CUSTOMER understands that there can be no assurance that any analysis of this nature will identify all possible vulnerabilities or propose exhaustive and operationally viable recommendations to mitigate this exposure.

15. Non-Solicitation:

Neither Party will directly solicit for employment any employee/contractor of the other Party performing Services under this Statement of Work, during the term of the relevant Statement of Work or for one year after the employee/contractor ceases performing Services.

Points of Contacts (POC) List

Project Personnel		Email	Telephone
Snohomish County Contacts / Stakeholder			
	Project Lead	Fred.Hartmann@snoco.org	(425) 388-3998
	Project Coordinator		
	Accounts Payable	DIS.Admin@snoco.org	
Emagined Security Contacts			
David Sockol	CEO	DavidSockol@emagined.com	(650) 593-9829
Paul Underwood	COO	PaulUnderwood@emagined.com	(801) 294-2917
Chris Odom	CRO – Project Management	ChrisOdom@emagined.com	(801) 923-1631
Brennan Egan	Account Manager	BrennanEgan@emagined.com	(480) 440-2146

Emagined Security

Clarity: Vulnerability Management Support

Experts in Managing & Supporting IT Cyber Security Operations

01 Scan
02 Assign
03 Remediate
04 Report & Analyze

Report Findings: ACME Sample Report - 2023

Severity	Title	Remediation Status
High	Excessive Privileges - Excessive Permissions	Open
High	Cross-Site Request Forgery (CSRF)	Open
Medium	Test Environment Externally Accessible	Open
Medium	IKE Aggressive Mode with PSK	Open
Informational	AutoComplete Enabled	Open

Enhanced Protection & Significantly Improved Security

All of this comes at a reasonable price that allows our clients to leverage our best practices, technology expertise, and scalable infrastructure.

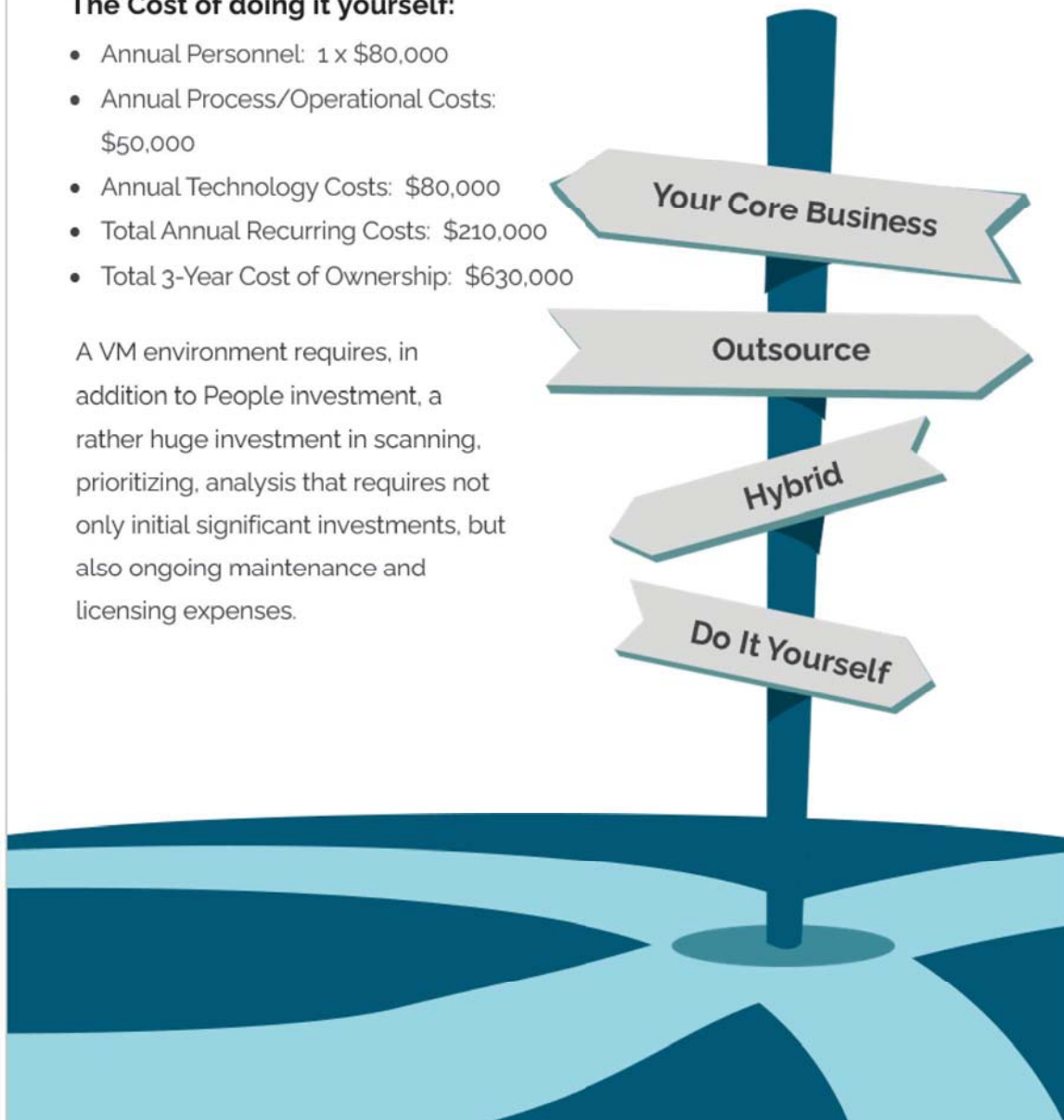
Emagined's Clarity: Vulnerability Management Support can be used to ensure that your organization knows what data is relevant and actionable. These capabilities provide new capabilities while maintaining overall cost effectiveness empowering our customers to focus on their core business.

Vulnerability Management Decisions, Decisions...

The Cost of doing it yourself:

- Annual Personnel: 1 x \$80,000
- Annual Process/Operational Costs: \$50,000
- Annual Technology Costs: \$80,000
- Total Annual Recurring Costs: \$210,000
- Total 3-Year Cost of Ownership: \$630,000

A VM environment requires, in addition to People investment, a rather huge investment in scanning, prioritizing, analysis that requires not only initial significant investments, but also ongoing maintenance and licensing expenses.





Let Us Do The Work

Emagined's Clarity: Vulnerability Management Support Services has the mechanisms in place to identify vulnerabilities and prioritize remediation efforts so you can focus on other critical areas of your business. By leveraging Emagined Security's extensive team of security experts and our Clarity solutions, clients will realize huge savings over performing Vulnerability Management services themselves.



Clarity Functions

- Broad assessment & coverage of over 62,000+ CVE
- White-glove setup and management
- Zero Day Checks
- Proactive & Perimeter focused
- Asset Discovery
- Network, Application, Cloud Infrastructure
- Visibility of the entire Attack Surface
- Most affordable "type" of assessment
- Continuous Attack Surface Checks
- Fastest turn-around on reporting/dashboard
- Track Remediation efforts online



Security Consulting Services

- Implementation Support
- Incident Response Level 2
- Managed Incident Response
- Remediation Support
- Penetration Testing
- Asset Tracking
- Vulnerability Management
- Managed Antivirus
- Managed APT Tool
- Managed Data Loss Prevention
- Managed Encryption
- Managed Perimeter Security
- Firewalls
- SPAM and Messaging Security
- Web Security
- Metrics Creation
- Formal Process Documentation
- Tool Enhancements

CALL US.

For a **free service consultation** you can contact us at: www.emagined.com or give us a call

Emagined's Clarity Vulnerability Management Support Brochure

Overview

Vulnerability Management has historically been a challenge and Clarity Vulnerability Management Support provides much needed transparency through a graphical interface that:

- Manages insights into the sheer volume of vulnerabilities
- Graphically prioritizes which vulnerabilities to remediate
- Tracks vulnerability and patch management status

Emagined Security's service brings focus to their core MSS capabilities while protecting the integrity an organizations security capability through our highly sophisticated Vulnerability Management Support knowledge offerings. Emagined Security services are designed to either utilize our customer's technology along with our solutions to help secure your environment.

Emagined Security's specialized security analysts work side by side with customer IT teams to give individualized guidance and support. Our Clarity addition further enhances offering this by leveraging the power of analytics to help organizations triage asset mitigation and response.

Benefits

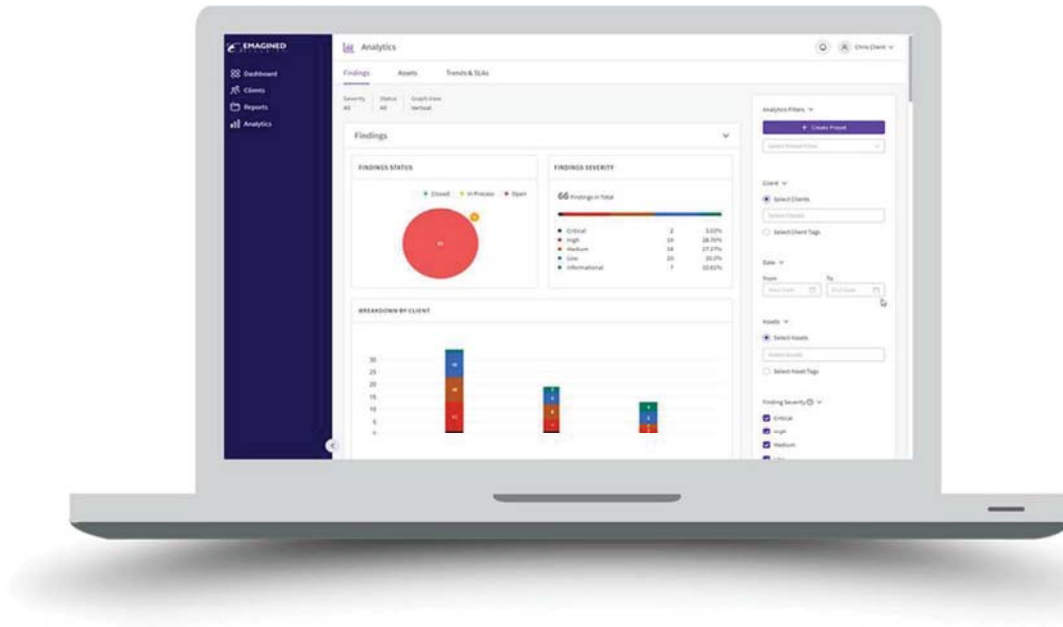
The evolution of information technology and security is a never-ending process. Emagined Security's Clarity Vulnerability Management Support has the mechanisms in place to identify risks early so you can focus on other critical areas of your business.

Emagined Security's Team has extensive experience helping its clients secure their network and web-enabled electronic commerce systems. We have helped many of the world's largest financial institutions protect their financial service delivery systems and have assisted a variety of vendors that offer electronic commerce solutions.


Description of Service





Clarity Vulnerability Management Support offers the services you need in a graphical manner that will empower your business.

Clarity Vulnerability Management Dashboards



Clarity Vulnerability Management Support can be used to ensure that your organization knows what data is relevant and actionable (Sample dashboards are shown below).



-  Dashboard
-  Clients
-  Assessments
-  Reports

Report Findings: ACME Sample Report - 2023

Clients > ACME > Reports > ACME Sample Report - 2023 > Findings Search & Re

Readout
Details
Narrative
Findings
Assets
Artifacts
Attack Path

19 REPORT FINDINGS

[Sort Options](#) [Report Logs](#)

<input type="checkbox"/>	Severity	Finding Title	Linked Ticket	Assigned To	Date Reported	Time To SLA	Status
<input type="checkbox"/>	High	Service Accounts - Excessive Permissions		patrickcleary@emagined.com	02-16-2023		Open
<input type="checkbox"/>	Medium	Cross-Site Request Forgery (CSRF)		patrickcleary@emagined.com	02-16-2023		Open
<input type="checkbox"/>	Medium	Test Environment Externally Accessible		patrickcleary@emagined.com	03-03-2023		Open
<input type="checkbox"/>	Medium	IKE Aggressive Mode with PSK		patrickcleary@emagined.com	02-16-2023		Open
<input type="checkbox"/>	Informational	AutoComplete Enabled		patrickcleary@emagined.com	03-04-2023		Open
<input type="checkbox"/>	Low	Cache Control Not Enabled		patrickcleary@emagined.com	03-24-2023		Open
<input type="checkbox"/>	Low	NTP Mode 7 Vulnerabilities Present		patrickcleary@emagined.com	02-17-2023		Open
<input type="checkbox"/>	Low	Debugging Enabled		patrickcleary@emagined.com	02-16-2023		Open
<input type="checkbox"/>	High	DLL Hijacking		patrickcleary@emagined.com	04-06-2023		Open

EMAGINED
SECURITY

- Dashboard
- Clients
- Assessments
- Reports
- Content Library
- Analytics
- Runbooks

Report Findings: ACME Sample Report - 2023

Clients > ACME > Reports > ACME Sample Report - 2023 > Findings

Finding Detail
✕

Service Accounts - Excessive Permissions

Report
ACME Sample Report - 2023

Description

The accounts used to manage services on the vulnerable assets are operating with excessive access control permissions.

The service accounts observed in use throughout the Client are configured to allow excessive permissions in its authorization (i.e. the authority to add, modify, and/or delete data regardless of data ownership) and connectivity (i.e. the number of systems the account may log into throughout the Client). An attacker could leverage this overly permissive policy to view, extract, damage or change data. Attacks of this nature could be realized by both insiders as well as external entities alike.

In addition to its failure to follow a 'least-privilege' access/trust model, the excessive permissions vulnerability also reduces the amount of effort an attacker would need to exert in order to gain access to data otherwise inaccessible were the permissions set appropriately for the comprised service account. That is, an attacker needs only compromise an application or service level account to access data rather than requiring the attacker to apply advanced techniques to first elevate local account privileges. This in essence can greatly reduce the number of steps or pivots an attacker needs to make to achieve the desired result.

As domain permissions are available to the service level accounts assigned to applications, it also becomes harder to track accountability were an incident to occur and the Client's security personnel were tasked with resolving who or what gained unauthorized access to the data.

NOTE: The list of vulnerable assets above is only representative of the Client environment. There may be other Client systems that leverage additional service accounts that Emagined Security did not detect/list due to the scope and time constraint of the on-site engagement and the volume of data collected. The Client is strongly encouraged to identify all applications using service accounts and validate the user and access permissions are set accordingly.

Specific details and screenshots of this issue redacted from the sample report.

Mitigation

Service accounts should be mapped to a specific application, so if the Client used two different applications, there should be two service accounts. Each service level account should be assigned operate under a 'least-privilege' trust model, where the minimum required permissions are set. In other words, if the service account does not require administrative access to the system, the administrative role should not be applied. Additionally, service accounts that

FINDING ID

STATUS
Open

SEVERITY
High

APPLICABLE

DATE REPORTED
02-16-2023

SOURCE
platform

TIME TO SLA
No SLAs Matched This Finding

TAGS

- include_url
- asset_sample_app_1
- scope_external_network

Assets For Client: Acme Company

Clients • Acme Company • Assets

Import Assets + New Asset

New Asset

Parent Asset
Select Optional Parent Asset

Asset Name
Office PC

Asset Type
Workstation

Asset Criticality
Medium

System Owner
Carter Jones

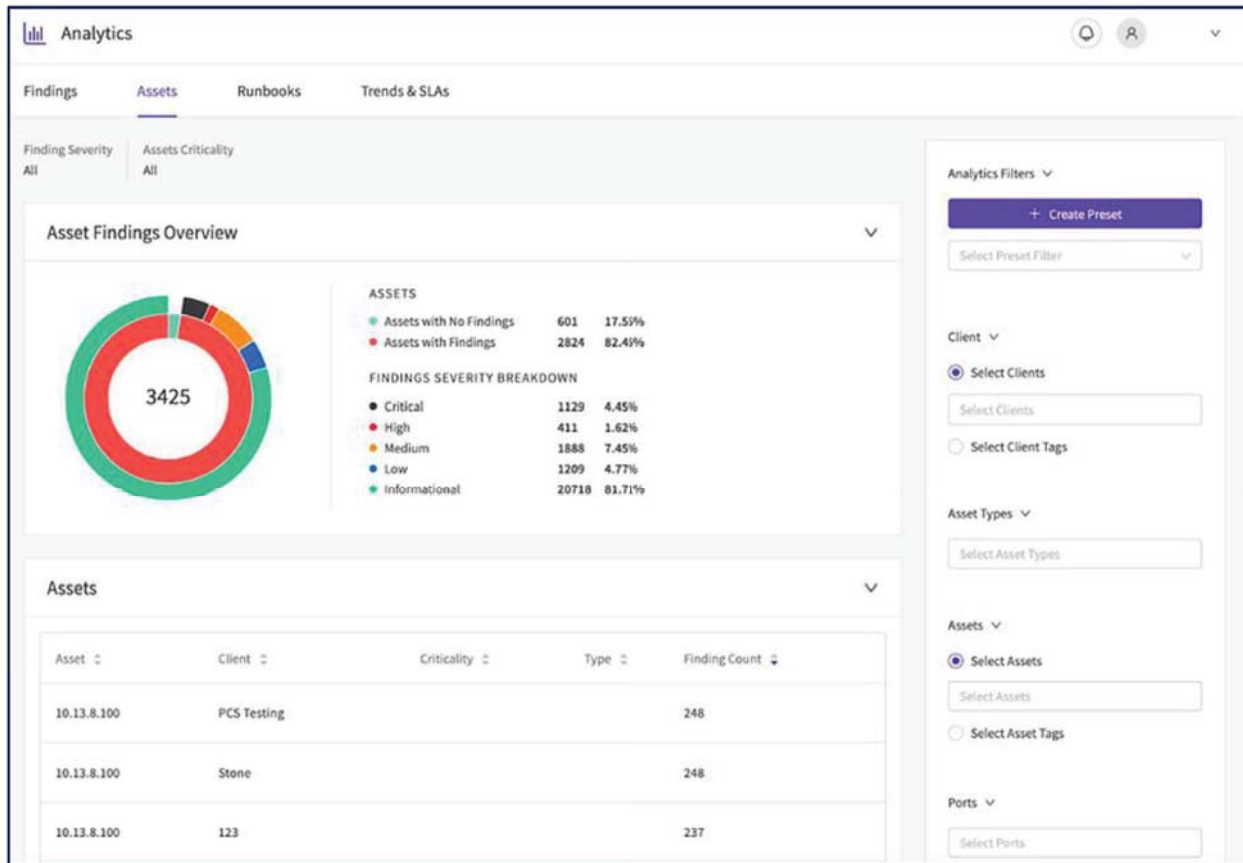
Data Owner

Hostname

Search...

Actions

- Search Edit Add Delete
- Search Edit Add Delete
- Search Edit Add Delete
- Search Edit Add Delete
- Search Edit Add Delete



Emagined Security offers its customers a comprehensive suite of real-time managed security services designed to enhance the information security posture of our customer’s networks through around-the-clock management and monitoring of security devices, analysis of their log data, and response to potential security threats.

EMAGINED SECURITY

Emagined Security

2816 San Simeon Way
San Carlos, CA 94070
650-593-9829
www.emagined.com

SCHEDULE B

MUTUAL NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement (“Agreement”), is by and between EMAGINED SECURITY, INC. (“EMAGINED SECURITY”), a California based Corporation, with offices at 2816 San Simeon Way, San Carlos, CA 94070 USA and SNOHOMISH COUNTY, a political subdivision of the State of Washington, with offices at 3000 Rockefeller Avenue, Everett, WA 98201.

It is recognized that it may be necessary or desirable to exchange information between the parties hereto for the purpose of discussing potential mutual business opportunities. With respect to the information exchanged between the parties subsequent to this date, the parties agree as follows:

1. Confidential Information

As used in this Agreement, "Confidential Information" shall include, but not be limited to, any information whether of a technical, business or other nature (including, without limitation, trade secrets, know-how and information relating to the technology, customers, business plans, promotional and marketing activities, finances and other business affairs) that is generally not known to the public originated by the disclosing party (“Discloser”), and received by the other party hereto (“Recipient”). Confidential Information may be contained in tangible materials, such as data, software, modules, components, designs, utilities, databases, subsets, objects, program listings, tools, models, methodologies, programs, systems, analysis frameworks, leading practices, report formats, manner of data expression and specifications, or may be in the nature of unwritten knowledge. In addition, Confidential Information includes all information that Recipient may obtain by walk-through examination of Discloser premises. Confidential Information also includes information which Discloser obtains from another party and which Discloser treats as proprietary or designates as Confidential Information, whether or not owned or developed by Discloser.

2. Use and Ownership of Confidential Information

Recipient, except as expressly provided in this Agreement, will not disclose Confidential Information to anyone without Discloser’s prior written consent. In addition, Recipient will not use, or permit others to use, Confidential Information for any purpose other than that for which it was disclosed. Recipient will take all reasonable measures to avoid disclosure, dissemination or unauthorized use of



EMAGINED SECURITY

Confidential Information. All Confidential Information will remain the exclusive property of Discloser, and Recipient will have no rights, by license or otherwise, to use the Confidential Information except as expressly provided herein.

3. Exceptions

The provisions of Section 2 will not apply to any Confidential Information that (i) is or becomes publicly available without breach of this Agreement; (ii) can be shown by documentation to have been, known to Recipient at the time of its receipt from Discloser; (iii) is rightfully received from a third party who did not acquire or disclose such information by a wrongful or tortious act; (iv) can be shown by documentation to have been independently developed by Recipient without reference to any Confidential Information, or (v) is required to be disclosed according to applicable law.

4. Disclosures to Governmental Entities

If Recipient becomes legally obligated to disclose Confidential Information by any governmental entity with jurisdiction over it, Recipient will give Discloser prompt written notice to allow Discloser to seek a protective order or other appropriate remedy. Such notice must include, without limitation, identification of the information to be so disclosed and a copy of the order. Recipient will disclose only such information as is legally required and will use its reasonable best efforts to obtain confidential treatment for any Confidential Information that is so disclosed.

5. Compliance with Laws; Exportation/Transmission of Confidential Information

Recipient will comply with all applicable federal, state, and local statutes, rules and regulations, including, but not limited to, United States export control laws and regulations as they currently exist and as they may be amended from time to time.

6. Return of Confidential Information

Upon request, the recipient immediately will return all tangible material embodying Confidential Information (in any form and including, without limitation, all summaries, copies and excerpts of Confidential Information).

7. Business Relationships

The undersigned shall not attempt to engage each other's clients introduced to each other in business that is exclusive to one party for a period of one year from the time work ends, unless there is a prior agreement between parties about a specific client.

8. Limited Relationship



EMAGINED SECURITY

This Agreement will not create a joint venture, partnership or other formal business relationship or entity of any kind, or an obligation to form any such relationship or entity.

9. Common Interest Agreement.

To the extent that any Confidential Information provided or made available hereunder may include material subject to the attorney-client privilege, work product doctrine or any other applicable privilege concerning pending or threatened legal proceedings or governmental investigations, Recipient and Discloser understand and agree that they have a commonality of interest with respect to such matters and it is their desire, intention and mutual understanding that the sharing of such material is not intended to, and shall not, waive or diminish in any way the confidentiality of such material or its continued protection under the attorney-client privilege, work product doctrine or other applicable privilege. All Confidential Information provided or made available by Discloser that is entitled to protection under the attorney-client privilege, work product doctrine or other applicable privilege shall remain entitled to such protection under these privileges, this Agreement, and under the joint defense doctrine. Nothing in this Agreement obligates Discloser to reveal material subject to the attorney-client privilege, work product doctrine or any other applicable privilege.

10. Cumulative Obligations

Recipient's obligations hereunder are in addition to, and not exclusive of, any and all of its other obligations and duties to Discloser, whether express, implied, in fact or in law.

11. Term and Termination

This Agreement is intended to cover Confidential Information disclosed by Discloser both prior and subsequent to the date hereof. Unless otherwise earlier terminated, this Agreement automatically will terminate upon the completion or termination of dealings between Discloser and Recipient; provided, however, that Recipient's obligations with respect to Discloser's Confidential Information will survive completion or termination of the dealings between the parties.

12. Nonwaiver

Any failure by Discloser to enforce Recipient's strict performance of any provision of this Agreement will not constitute a waiver of Discloser's right to subsequently enforce such provision or any other provision of this Agreement.

13. Governing Law; Etc.



EMAGINED SECURITY

This Agreement shall be governed by, construed and enforced in accordance with the laws of the State of Washington, U.S.A., and may be executed in counterpart copies. Each party hereby waives its right to a jury trial for any claims that may arise out of this Agreement. If a provision of this Agreement is held invalid under any applicable law, such invalidity will not affect any other provision of this Agreement that can be given effect without the invalid provision. Further, all terms and conditions of this Agreement will be deemed enforceable to the fullest extent permissible under applicable law, and, when necessary, the court is requested to reform any and all terms or conditions to give them such effect.