



Emagined Security
2816 San Simeon Way
San Carlos, CA, 94070

Phone: (650) 593-9829
www.emagined.com

February 17, 2021

Charleen Patten
Washington State Auditor's Office
3200 Sunset Was S.E.
PO BOX 40031
Olympia WA 98504-0031
E-mail Address: contractmanager@sao.wa.gov
Telephone Number: (564) 999-0941
RE: RFP K646-RFQQ-2011; Security Assessment Services

Dear Charleen,

We at Emagined Security are delighted to respond to Washington State Auditor's request to provide Security Assessment Services. We are committed to providing our best resources to this and every engagement performed for your company as we build a relationship with you as your partner in information security.

Our goal is to earn your trust and deliver security services at the highest levels. Our ability to continuously earn the trust of our clients and exceed expectations in delivery is what raises Emagined Security above the competition and is demonstrated by our clients repeatedly turning to us for assistance. We are proud of what we have accomplished in partnership with our existing clients and look forward to providing the same high level of services to you. If you have any questions regarding this response, please contact me at (650) 593-9829.

Very truly yours,

David Sockol
President & CEO



Proposal for

Security Assessment Services

Prepared For:

WASHINGTON STATE AUDITOR IN RESPONSE TO RFP
K646-RFQQ-2011

FEBRUARY 17, 2021

Prepared By:

The Emagined Security Consulting Team

Compiled By:

David Sockol
President & CEO
Emagined Security
2816 San Simeon Way
San Carlos, CA 94070
650-593-9829

TABLE OF CONTENTS

SECTION I – LETTER OF SUBMITTAL – Mandatory Required (MR)(PASS/FAIL) ...	4
A. ORGANIZATION SUMMARY (MR)	4
B. BUSINESS IDENTIFICATION (MR)	5
C. COMPANY OFFICERS (MR)	5
D. PRIMARY CONTACT (MR)	6
E. LEGAL STATUS (MR)	6
F. FORMER EMPLOYEE STATUS (MR)	6
G. OMWBE STATUS (MR)	6
H. CONTRACT TERMINATIONS (MR)	7
I. TAX INFORMATION (MR)	7
J. SUBCONTRACTOR QUALIFICATIONS (MR)	7
K. STATEMENT OF ACCEPTANCE OF TECHNICAL REQUIREMENTS (MR) .	8
L. COMPLIANCE WITH INSURANCE REQUIREMENTS (MR)	8
SECTION II – QUOTATIONS SECTION MANDATORY REQUIRED (MR) (SCORED)	8
A. COST PROPOSAL (MR)	8
B. COMPUTATION	13
SECTION III – QUALIFICATIONS SECTION (MR) (SCORED)	13
SECTION III-a – QUALIFICATIONS SECTION (Optional and separate from Section III)	24
SECTION IV – CUSTOMER REFERENCES (MR)(PASS/FAIL)	26
SECTION V – RESUMES (MR) (SCORED)	26
SECTION VI – CERTIFICATIONS AND ASSURANCES (MR)(PASS/FAIL)	27
SECTION VII – REPORT SAMPLES (MR)(PASS/FAIL)	29
SECTION VIII – SECURITY QUESTIONNAIRE (MR)(PASS/FAIL)	32
SECTION IX – CONFIDENTIALITY AND NONDISCLOSURE AGREEMENT, (MR)(PASS/FAIL)	35
SECTION X – PROCUREMENT EVALUATION FOR EXECUTIVE ORDER 18-03 CERTIFICATION FORM (MR) (Scored)	37
ATTACHMENT 1: Section V – Resumes	39
ATTACHMENT 2: Sample Report	40
ATTACHMENT 3: Detailed Penetration Testing Methodology	41



EMAGINED SECURITY

SECTION I – LETTER OF SUBMITTAL – Mandatory Required (MR)(PASS/FAIL)

REQUEST

A. ORGANIZATION SUMMARY (MR)

The proposer must provide a summary of the organization/firm/individual's pertinent expertise, skills, client base and services that are available for this project.

RESPONSE

In response to RFP K646-RFQQ-2011, Emagined Security services offered in this proposal concentrate on Emagined Security's support for the technology assessment needs of the business functions of Washington State Auditor. In working with Washington State Auditor, we will begin by focusing on your internal needs first.

Emagined Security specializes in:

Web Application Penetration Testing, API Penetration Testing, SCADA Penetration Testing, External Infrastructure Ethical Hack, Internal Infrastructure Ethical Hack, Mobile Code Penetration Test, Wireless LAN Penetration Test, Application Ethical Hacking, and Source Code Review

Emagined Security's dedicated penetration test team has many security certifications, are frequent presenters at security conferences, have testified in front of state congresses.

Emagined Security understands the scope and magnitude of the engagement proposed by the Washington State Auditor and has an extensive staff with penetration testing experience that will be able to assist with the up to twelve (12) state agencies and up to twelve (12) local government penetration tests required to complete over the approximately two (2) year contract as requested. We further understand that this contract may be extended up to three (3) years as requested and negotiated.

Emagined Security's commercial clients cover a wide range of U.S. and global Fortune 500 organizations, including the government, financial services, energy, healthcare, high tech, manufacturing, & insurance industries.

The company is comprised of 40 senior information security professionals in the industry, with an average of 15+ years of experience. Consultants have varied and diverse backgrounds in information security with high levels of knowledge, industry certifications and practical experience.

Emagined Security was created to offer corporations a comprehensive array of sophisticated, adaptive security solutions that include both consulting and managed services. In support of this initiative, Emagined Security has built a highly talented organization specializing in information security consulting. The Company focuses on securing business solutions by providing a full complement of proactive, real-time, reactive, executive advisory, license advisory and support security services to global institutions, major corporations, and other smaller organizations, while providing a fully business-driven approach.

Emagined Security is the leading professional services provider for Information Security & Compliance solutions. Emagined Security empowers its clients to help them effectively manage IT risk in today's dynamic business environment. With deep industry and domain expertise, a proven track record, and by employing well known and respected



EMAGINED SECURITY

individuals from the Information Security community, Emagined Security can scale quickly and efficiently to provide clients with the rapid response required by best-in-class organizations.

REQUEST

B. BUSINESS IDENTIFICATION (MR)

The proposers must provide an overview of their firm/organization, including, but not limited to the following:

- *Organization/firm's name, address and main business location*
- *The location of the facility from which the proposer would operate, including the telephone, fax and e-mail address*
- *Organization/firm's start-up date.*

RESPONSE

Emagined Security, a privately owned and operated company, has been helping organizations with their security needs with an excellent track record of success since 2002.

Headquarters and Main Operating Address:

Emagined Security, Inc.
2816 San Simeon Way
San Carlos, CA 94070
650-593-9829 direct
david@emagined.com

REQUEST

C. COMPANY OFFICERS (MR)

The proposer must provide the names, addresses, and telephone numbers of principal officers (President, Vice President, Treasurer, Chairperson of the Board of Directors, etc.).

RESPONSE

David Sockol: CEO, Board of Directors

650-593-9829 direct
david@emagined.com

Paul Underwood: COO, Board of Directors

801-294-2917 direct
paulunderwood@emagined.com

Julianna Sockol: Chairman, Board of Directors

650-799-6206 direct
js@emagined.com

REQUEST



EMAGINED SECURITY

D. PRIMARY CONTACT (MR)

The proposer must include who within the firm/organization will have prime responsibility and final authority for the work under the proposed contract. Include the following:

- Name
- Title or position
- Address
- E-mail address
- Telephone and fax numbers.

RESPONSE

David Sockol: CEO, Board of Directors

2816 San Simeon Way

San Carlos, CA 94070

650-593-9829 direct

davidsockol@emagined.com

REQUEST

E. LEGAL STATUS (MR)

The proposer must specify the legal status of the Organization/Firm (sole proprietorship, partnership, corporation, etc.) and the year the entity was organized to do business as the entity now exists.

RESPONSE

Emagined Security, Inc.

Legal Status: Corporation

LLC Formed in 2002

Incorporated in January 30, 2007

REQUEST

F. FORMER EMPLOYEE STATUS (MR)

*If any employee of the proposer was an employee of the State of Washington or a Washington local government during the **past 24 months**, or is now an employee of the State of Washington or Washington local government, identify the individual by name, state agency or local government previously or currently employed by, job title or position held and separation date.*

RESPONSE

None – Emagined Security does not employ any former State of Washington individuals.

REQUEST

G. OMWBE STATUS (MR)

Minority and women-owned businesses are encouraged to participate. Please identify if the contractor or any subcontractors are a minority and women-owned business. Please provide the OMWBE certification number.



EMAGINED SECURITY

RESPONSE

Emagined Security is a certified small business but is not an OMWBE.

REQUEST

H. CONTRACT TERMINATIONS (MR)

If the proposer has had a contract terminated for default in the past five years, describe such incident. Termination for default is defined as notice to stop performance due to the proposer's nonperformance or poor performance. Issue of performance may have been:

- *Not litigated due to inaction on the part of the proposer, or*
- *Litigated and such litigation determined that the proposer was in default.*

Proposers will submit full details of the terms for default. Proposers will identify the other party, its name, address, and phone number, and present the proposer's position on the matter. The State Auditor's Office will evaluate the facts and may, at its sole discretion, reject the proposal on the grounds of the past experience.

If the proposer has experienced no such termination for default in the past five years, so indicate.

RESPONSE

None – Emagined Security has not had any terminations for default in the past five years.

REQUEST

I. TAX INFORMATION (MR)

The proposer must provide its Federal Employer Tax Identification number and the Washington Uniform Business Identification (UBI) number issued by the State of Washington Department of Revenue.

RESPONSE

Tax Number: 01-0677102

UBI: 603 010 821

REQUEST

J. SUBCONTRACTOR QUALIFICATIONS (MR)

For each subcontractor, the proposer must address the submittal questions set forth in A – C and E – I above.

The proposer must include a statement that if awarded the contract as the primary contractor, the proposer will accept full responsibility for successful performance of the entire scope of work.

RESPONSE

Emagined Security will not be using any subcontractors in delivering this effort. We accept full responsibility for successful performance of the entire scope of work.



EMAGINED SECURITY

REQUEST

K. STATEMENT OF ACCEPTANCE OF TECHNICAL REQUIREMENTS (MR)

The Letter of Submittal will include a statement that the proposer accepts all of the elements and requirements identified in Section III, Qualifications Section, and be signed by the principal, partner or appropriate obligating authority.

RESPONSE

Emagined Security accepts all of the elements and a requirement identified in Section III, Qualifications Section and is signed by the principal, partner or appropriate obligating authority.

REQUEST

L. COMPLIANCE WITH INSURANCE REQUIREMENTS (MR)

Each proposer must indicate in the Letter of Submittal and, as a condition of contract award, that it will submit to the State Auditor's Office within 15 days of the contract effective date, a certificate of insurance which outlines the coverage and limits as defined in the Insurance section.

RESPONSE

Upon award, Emagined Security will work with the state to ensure we comply with mutually agreed upon insurance requirements and provide a certificate of insurance.

I hereby sign this letter of submittal per the RFP requirements:

David Sockol
President & CEO

17 February 2021

SECTION II – QUOTATIONS SECTION MANDATORY REQUIRED (MR) (SCORED)

REQUEST

A. COST PROPOSAL (MR)

The State Auditor's Office requires two price quotes for this RFQQ. 1) Proposers must provide a single, not-to-exceed, "blended hourly rate" price quote for the contract term. Proposers shall be bound by the hourly rate they quote in this RFQQ. The rates quoted will be considered "not-to-exceed" rates. 2) Because the specific state agencies are not identified, bidders are instructed to provide a bid (price quote) for the sample state agency listed below as well.

Proposers must consider the following when completing the Price Proposal:

- *Overtime rates are not allowed.*

- *Quote all-inclusive rates in United States dollars to include travel and all expenses to accommodate working with State Auditor's Office. Consultants are required to collect and pay Washington State taxes as applicable.*

RESPONSE

Price Quotes (Blended Rate)

Emagined Security has a blended rate for performing the above services at \$160 per hour including all travel and related costs to the penetration testing. Since Emagined Security will not be reimbursed for any travel, all requests for travel must be approved by Emagined Security and require a minimum of 4 weeks' notice.

Emagined Security will work with the State of Washington to ensure the scope meets the appropriate budget appropriated from the State of Washington.

Price Quotes (Sample Agency)

Emagined Security has reviewed the scope listed for the "Sample Agency" and has provided the below costing (*Scoping Based Upon Information from Amendment 1*).

Based on the scope provided Emagined Security has estimated the following for performing the audit on the sample agency:

- Costing below is based on the updated scoping provided in Amendment 1.
- Applications and networks are based on level 1 testing since no demonstrations of applications provided.

Budget				
The following budget is for the sample agency:				
	<i>Description / Task</i>	<i>Est. Hours</i>	<i>Unit Cost</i>	<i>Total</i>
1	<i>Internal Application Penetration Test – (6 defined applications per instructions) Bid at Level 1 application Tier without demo</i>	192	160	\$30,700
2	<i>Internal Network Penetration Test - 1,000 WS IPs, 85 svrs, 50 multi-fuunction devs</i>	60	160	\$9,600
3	<i>External Application Penetration Test (est. 2 apps & 1 public website)</i>	40	160	\$6,400
<i>SAO shall pay an amount up to but not to exceed \$46,720 for audit services unless a change order is authorized</i>				\$46,720

REQUEST

The Proposal must contain a comprehensive description of services including the following elements:

- *Project Approach/Methodology (MR) – Include a complete description of the proposed approach and methodology for completing the testing, performing the analysis and preparing the report.*

The evaluation process is designed to award a contract to the Consultant(s) whose proposal best meet the requirements of this RFQQ.

RESPONSE

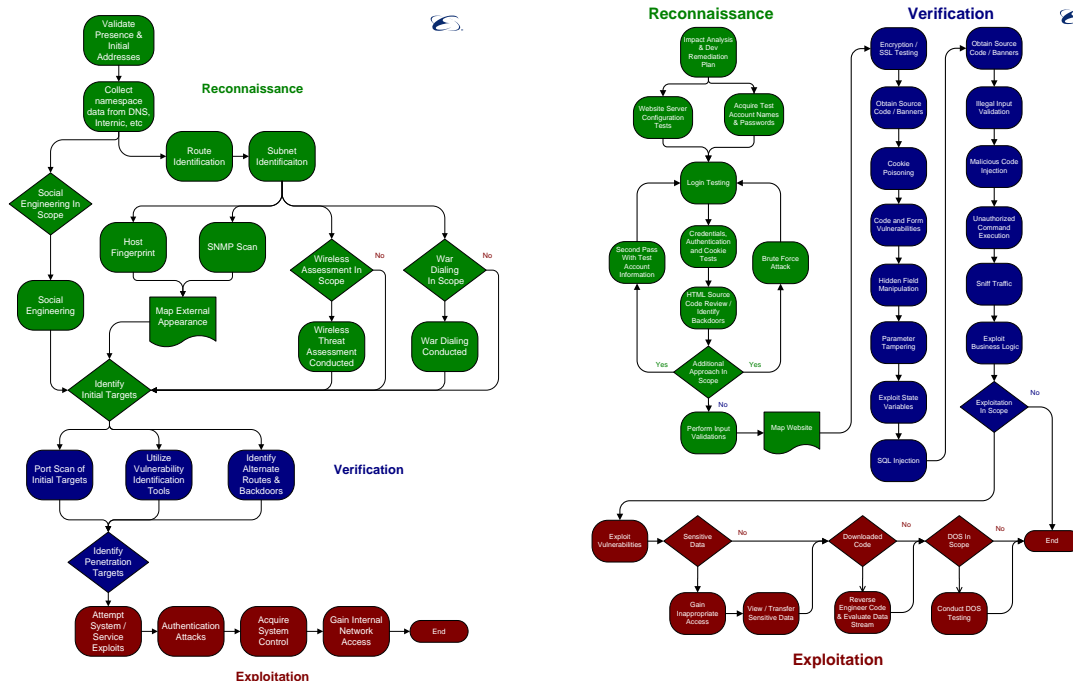
Project Approach

When working with other organizations, Emagined Security takes pride in ensuring we do not interrupt the general schedules of state or organization employees. Emagined Security would request that State Auditor Office employee's setup initial meetings with prospective organizations and Emagined Security will take ownership or relationships and keep state auditor office employees informed on requirements of the State to assist Emagined Security in completing tasks.

Emagined Security utilizes a proven project management methodology that allows us to consistently monitor project status, budgets and quickly escalate and resolve issues. Emagined Security has performed similar engagement for other State agencies such as the State of Colorado along with over a hundred Cities and Agencies around the country. Details can be found in the *Management approach, methodology and implementation strategies for managing and delivering their product* Section on page 22.

Project Methodology

This section contains a general outline of the procedures to complete a vulnerability assessment / penetration test / ethical hack. The project Methodology for penetration testing consist with following a framework based on OWASP. Emagined Security additionally enhances the recommendations on OWASP penetration testing by determining business factors that are important to the application and organization being testing, ensuring The Emagined Security testing is performed with diligence and direction that is comprehensive, meaningful, and directed to the organization and application being tested.



These flow charts cover Emagined Security's Penetration Testing methodology at a high level; it does not enumerate the specific steps included in our procedures. Penetration tests are broken into three phases. While each phase is separate, not all phases are independent of each other. Some activities such as avoiding detection are listed as a separate phase, but they in reality typically also occur during all other phases of a test.

Emagined Security has included a detailed methodology for our Penetration testing service in Attachment 3 if additional details are desired.

REQUEST

The Proposal must contain a comprehensive description of services including the following elements:

- *Work Plan (MR) – Include all project requirements and the proposed tasks, services, activities, etc. necessary to accomplish the testing in the scope of the project defined in this RFQQ. This section of the technical proposal must contain sufficient detail to convey to members of the evaluation team the proposer's knowledge of the subjects and skills necessary to successfully complete the testing for this project. Include any required involvement of State Auditor's Office staff.*

The evaluation process is designed to award a contract to the Consultant(s) whose proposal best meet the requirements of this RFQQ.

RESPONSE

Work Plan

Initially Emagined Security will meet with the State of Washington SAO and the entity or agency under audit and help determine a proper scope for the penetration testing to be performed under the audit. Emagined Security will attend meetings with both organizations to help scope out what opportunities for penetration testing are available. Emagined Security will also support the State of Washington SAO with explanations of the penetration testing to be performed to the entity or agency being audited to help them understand the goals, risks and rewards of performing the penetration testing through the State of Washington SAO audit.

Additionally, the workplan will be defined in the State of Washington SAO office Rules of Engagement that will lay out the applications, dates and contacts of the organization to be tested. This workplan will expand to include the dates/times, contacts and communication to be provided during the penetration testing.

The Workplan will include specifics on escalation of identified vulnerabilities, how communications channels are defined and will provide the comprehensive details of each application being tested.

Each test is designed based upon the requirements and desires of the SOA (documented in the ROE). As such, before the penetration test begins the SOA and Emagined Security agree upon several test parameters. These include:

- *Attacker Persona:* Will the penetration test mimic the actions of an outsider to the company, or a company employee, or some combination? For those studies coming from the outside efforts will center on only Internet connectivity, or will efforts such as partner locations be used as points to the network?
- *Methods Allowed:* The exact types of methods should be enumerated. This includes whether certain classes of attacks (e.g., Buffer Overflows, Denial of Service (DoS)) will be used.
- *Access to Results:* Who has access to the results of the test must be agreed upon beforehand. This also will limit those individuals that can be present during the actual test. (See monitoring below)

- *Systems Allowed:* This will identify the systems being tested and enumerate those specific systems that are “off limits” and cannot be tested.
- *Monitoring:* Complete logs of all activities must be kept and made available to the client. This also includes if the client must be present during all activities.
- *Professional Manner:* Company should require persons conducting test to act in a professional manner, meaning that they will not try attacks known to violate parameters established in the methods section and adhering to the C|EH or OSCP rules. Unprofessional conduct includes using known DoS attacks when DoS attacks have specifically been excluded.
- *Social Engineering:* Emagined Security does not routinely conduct “social engineering” attacks on customer support organizations because those are typically highly destructive. Emagined Security will work with a customer to design an assessment program that measures vulnerability to a social engineering attack without performing the deceitful activities commonly referred to as social engineering.

REQUEST

The Proposal must contain a comprehensive description of services including the following elements:

- *Project Schedule (MR) – Include a project schedule indicating when the testing would be completed and when deliverables, would be provided. Bidders will consider that documentation detailing the testing completed to identify issues, including screen shots as necessary, is required to support the detailed testing results communicated to agencies.*

The evaluation process is designed to award a contract to the Consultant(s) whose proposal best meet the requirements of this RFQQ.

RESPONSE

Project Schedule

The project scheduled is defined initially by the State of Washington SAO office Rules of Engagement that will lay out the applications, dates and contacts of the organization to be tested. This workplan will expand to include the dates/times, contacts and communication to be provided during the penetration testing. Each test is independently scheduled in the number of man weeks to perform a test. As multiple penetration testers may be assigned to an engagement, these tasks may overlap in calendar weeks. A sample schedule may look like the following:

Description / Task (Sample)	Duration
Application Penetration Test	2 Weeks
Internal Network Penetration Test	1 Week
External Network Penetration Test	1 Week
Configuration Review	1 Week
Reporting Time	1 Week
Time From Initial to Report	6 Weeks

REQUEST

The Proposal must contain a comprehensive description of services including the following elements:

- *Deliverables (MR) – Fully describe content and format of deliverables to be submitted under the proposed contract.*

The evaluation process is designed to award a contract to the Consultant(s) whose proposal best meet the requirements of this RFQQ.

RESPONSE

The deliverables 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.

Additional details can be found in *SECTION VII – REPORT SAMPLES*. A full sample deliverable can be found in Attachment 2.

REQUEST

B. COMPUTATION

The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. This means that the overall score for the cost proposal will account for the robustness of the proposer's qualifications as well as their proposed price. We will include both the blended hourly rate and the price quote in scoring the cost proposal. The cost proposal will be worth up to 10 percent of the total possible points – see the table in Chapter 4.4 of this RFQQ.

RESPONSE

Emagined Security has a blended rate for performing the above services at \$160 per hour including all travel and related costs to the penetration testing.

SECTION III – QUALIFICATIONS SECTION (MR) (SCORED)

REQUEST

The Qualifications Section of the proposal must contain information that will demonstrate to the evaluation committee the Firm/Staff understanding of the types of services proposed, the ability to accomplish them, and the ability to meet tight timeframes. Firm experience will be scored based on the capacity and experience of the firm to perform work similar to the tasks described in this RFQQ. Staffing will be scored

on how the proposer staffs the project to perform work similar to the tasks described in this RFQQ, including the number of staff and the mix or make of the team and their various levels of experience.

RESPONSE

Emagined Security will afford the SOA the ability to choose the level of each test we perform in order to ensure that assessment depth is appropriate for the associated risks. In this section the versions of the test will be referred to as Penetration Tests. Each test will be a mix of principal, senior, and general level penetration testers.

Based upon the sample organization provided, Emagined Security would staff this as follows:

- 1 Penetration Test Coordinator – Will provide scheduling and reviews of scoping, ROE creation and coordination to ensure that the lead penetration tester can meet the engagement obligations
- 1 Project Lead / Principal Penetration Test Lead (with OSCP / OSWE Certification) – Will provide day-to-day coordination of the penetration test objectives and ensure that that ROE and scope are consistently met. Additionally, daily communications are handled by the lead to ensure that agency objectives are met, and any critical or high vulnerabilities are address in a timely manner
- 2 Senior Web Application Penetration Testers (with OSCP / CEH Certification) – Will provide web application and thick client application testing
- 1 Web Application Penetration Tester (with minimum CEH Certification) – Will handle static external web application
- 2 Network Penetration Testers (with minimum CEH Certification) – Will perform internal and external penetration testing

Emagined Security employees over a dozen penetration testers and can staff multiple engagements of this size simultaneously. This is a dedicated penetration test team and all current members have been background checked by the State of Washington including CJIS certification and undergone fingerprint background checks. Sample Resumes can be found below in Attachment 1.

REQUEST

Recent experience with both government and private industries is a plus for both firm experience and staffing. Describe Vendor's experience and qualifications (in terms of Firm Experience and Staffing), especially with respect to performing work similar to the tasks described in this RFQQ. Provide experiences comparable to:

- *Vulnerability Assessments: Demonstrated experience in leading and/or participating in vulnerability assessments that include web applications, network, and source code. Qualifications could include at least one or more of the following certifications: Global Information Assurance Certification (GIAC), Web application Penetration Tester (GWAPT), Offensive Security Certified Professional (OSCP), Certified Ethical Hacker (CEH);*

In scoring this section, SAO may favor those Vendors describing experience providing services to state agencies or local governments.

RESPONSE

Although Emagined Security has performed penetration testing for the State of Washington, we have continued to expand our presence in other government entities as



well as other cities, states and auditor agencies over the course of our incorporation. These include Cities and agencies in Texas, Arizona and California. Emagined Security has a good balance of government to private industry clients. Including high tech clients in both the Bay area and the Silicon Slopes area of Utah.

Emagined Security performs hundreds of Web Application Penetration Tests, Network Penetration Tests, API & Mobile Penetration tests, Vulnerability Assessments and Wireless Assessments every year and it remains a core service Emagined Security offers. High level descriptions of some of the engagements are listed in each employee resume provided. Additionally all Emagined Security Penetration Testers hold FBI background checks to handle CJIS information, including the in the State of Washington.

Emagined Security ethical hackers possess a variety of certifications including but not limited to: Certified Information Systems Security Professional (CISSP), C|EH, InfraGard, Offensive Security PWB (OSCP), Thales nCSE, A++ Certification, Systems Security Certified Professional, Certified Computer Examiner, EnCase Certified Examiner, A+ Certified Service Technician, Server+ Certified, HP Accredited Platform Specialist – Proliant (APS), Microsoft Certified Professional Systems Engineer (MCSE), Certified in Homeland Security – Level 3 (CHS-III)*, GIAC Certified Firewall Analyst (GCFW)*, GIAC Security Essentials Certification (GSEC)*, Cellebrite UFED Certified – Mobile Devices (C00028), Cellebrite UFED Physical Certified – Mobile Devices (P00169), Securing Solaris – The Gold Standard (GGSC), Katana Forensics Lantern iOS First Responder Certification, Katana Forensics Laboratory iOS/Mac OS X Certification, GIAC, Certified Forensic Analyst (GCFA) 2014, DoD Clearances, Cisco Certified Networking Professional Security Specialist 1, Cisco Certified Networking Professional + Security (CCNP + Security), Check Point Certified Security Administrator (CCSA), Cisco Certified Networking Professional (CCNP), Cisco Certified Network Associate (CCNA), Microsoft – Microsoft Certified Professional, Systems Engineer, & Trainer, Novell – Certified Novell Administrator, Engineer, & Instructor, Project Management Institute – Project Management Professional, International Information Systems Security Certification Consortium (ISC)², ES – Enterasys Dragon Certification, State of California Peace Officer Standards and Training (P.O.S.T.) Level II, Member High Technology Crime Investigation Association (H.T.C.I.A.)

REQUEST

Recent experience with both government and private industries is a plus for both firm experience and staffing. Describe Vendor's experience and qualifications (in terms of Firm Experience and Staffing), especially with respect to performing work similar to the tasks described in this RFQQ. Provide experiences comparable to:

- *Wireless: Demonstrated experience in auditing and assessing federated wireless networks. Qualifications could also include GIAC Assessing and Auditing Wireless Networks (GAWN);*

In scoring this section, SAO may favor those Vendors describing experience providing services to state agencies or local governments.

RESPONSE

Emagined Security Consultants have performed wireless penetration tests in over 60 countries around the world including at the State of Washington, State of California and the State of Colorado. Emagined Security consultants have also been brought in as guest lecturers at the University of Utah on Wireless penetration testing. Additionally, some Emagined Security consultants have extensive wireless engineering backgrounds to

include the construction of the first Wireless ISP in the state of Utah over 15 years ago. Emagined Security consultants are WiFu certified wireless network penetration test specialists. Emagined Security's methodology goes beyond the GAWN methodology and include the following but are not limited to:

- 802.11 testing
- 802.11 Fuzzing Attacks
- Bluetooth
- DECT
- DoS on Wireless Networks
- Rogue Networks
- Securing and Configuring Wireless Clients
- Sniffing Wireless
- TKIP
- WLAN Auditing Methodologies
- WLAN Intrusion Detection Technology
- WPA2
- Zigbee

Wireless Network Penetration Testing

Emagined Security's methodology consists of the initial wireless penetration testing effort being performed using no knowledge of locations wireless network. Before executing the subsequent wireless penetration testing effort, the end user department will provide network configuration and product information to Emagined Security. Emagined Security will inform the department representative of the times during which scans will be conducted using the following two-phased approach.

Phase 1: Blind wireless LAN assessment

Given no information about the wireless network (and not using social engineering), CONSULTANT will perform the following Penetration Test:

- Identify the presence of a wireless WAP/LAN and operating frequency
- Connect to access point
- Impersonate an access point
- Capture information transmitted over the air
- Decrypt and read transmitted information
- Further map/identify internal network
- Gather information from client computer

Phase 2: Wireless LAN assessment

Given network configuration and product information, Emagined Security will attempt to perform the following tasks:

- Identify the presence of a wireless WAP/LAN and operating frequency
- Identify the components and network from outside of the physical office
- Connect to access point
- Impersonate an access point
- Capture information transmitted over the air (confirm encryption)
- Decrypt and read transmitted information (analyze traffic to map other network components)
- Further map/identify internal network
- Gather information from client computer

REQUEST

Recent experience with both government and private industries is a plus for both firm experience and staffing. Describe Vendor's experience and qualifications (in terms of Firm Experience and Staffing), especially with respect to performing work similar to the tasks described in this RFQQ. Provide experiences comparable to:

- *Non-invasive penetration testing experience of production environments, or identically structured pre-production or test environments, containing highly sensitive information. Qualifications should include: Web application Penetration Tester (GWAPT), Offensive Security Certified Professional (OSCP), Exploit Researcher and Advanced Penetration Tester (GXPN); and*

In scoring this section, SAO may favor those Vendors describing experience providing services to state agencies or local governments.

RESPONSE

Emagined Security performs hundreds of Vulnerability Assessments every year including at the State of Washington local government agencies, cities and county administrations. Many penetration tests are performed on production web applications that require sensitivity to ensure that applications are not taken offline during the testing. To ensure that sensitive production applications are not impacted by penetration testing, Emagined Security does limited automated penetration testing with specific, tested configurations created by Emagined Security to not impact production capabilities. Emagined Security's penetration testing is additionally thorough and finds many vulnerabilities that just running a "tool" does not uncover.

Emagined Security's methodology in this case is very similar to the methodology presented above with limited automated scanning and a majority of our exploit phases removed.

Additionally, Emagined Security performs selected manual testing of these applications designed to ensure they do not pose a risk to systems that may go offline due to improper testing.

Emagined Security has been successfully testing production systems with manual testing, designed by Emagined Security, to ensure that applications are not impacted during the testing. Emagined Security's manual testing methodology is extensive to ensure that applications are tested comprehensively without impacting performance.

Some of Emagined Security's experience in performing these tests are:

- *Emagined Security has performed Penetration Testing for several Cities and Counties in The State of Washington*
- *Emagined Security has performed Penetration Testing for several Cities in The State of California*
- Emagined Security has tested CJIS certified applications and networks where exposure of this data could cause major impact to law enforcement.
- Emagined Security has performed SCADA testing, remotely with successful results and comprehensive testing with no outages.
- Emagined Security has performed testing on production web applications for eCommerce while in production and processing thousands of transactions per minute.
- Emagined Security has tested credit card networks that require 99.99995 uptime requirements ensuring that no downtime was incurred during the testing
- Emagined Security has tested financial applications where loss of transactional information would have resulted in large financial losses for the customer we tested.

- Emagined Security has tested Certificate validation systems where the loss of OCSP connectivity would have resulted in the inability to validate highly sensitive certificates in production.
- Emagined Security has tested mainframe applications (without causing outages) where causing an outage could impact state usage of traffic systems.

These are just some examples of production testing performed by Emagined Security without taking a system offline.

Emagined Security ethical hackers possess a variety of certifications that have been previously listed above.

REQUEST

Recent experience with both government and private industries is a plus for both firm experience and staffing. Describe Vendor's experience and qualifications (in terms of Firm Experience and Staffing), especially with respect to performing work similar to the tasks described in this RFQQ. Provide experiences comparable to:

- *Expert-level knowledge of complex network design and architecture.*

In scoring this section, SAO may favor those Vendors describing experience providing services to state agencies or local governments.

RESPONSE

Emagined Security performs hundreds of assessments including reviewing complex network designs and architectures every year. Our consultants have been performing architecture reviews and creating complex secure networks for over 28 years (since 1993). Additionally, expert knowledge is required of network and web application architecture to ensure the sensitive data flow of information in organizations is protected during the lifecycle of the data.

Emagined Security, when necessary, provides expertise reviewing customer architecture and data flow(s) to ensure customers understand the appropriate methods of security their digital information wherever it is transported.

After engagements complete, Emagined Security continues to answer questions regarding previous penetration tests for several months / to a year to ensure state entities and agencies can remediate from vulnerabilities and feel comfortable with their security posture.

REQUEST

The Vendor must describe at least five (5) representative projects the Vendor has performed for customers during the three (3) years preceding the Proposal due date. Describe completed projects only; projects where the services are in the process of being put in place will not satisfy this requirement. The Vendor and their key team members must have had primary responsibility for the various phases of the projects including analysis, testing, document review, and implementation and reporting. Do not exceed two (2) typewritten, single-sided pages for each project's description. Each description should include, at a minimum, the project's purpose (i.e., Project Statement), the project's deliverables, the project's duration, and the results.

Scores for this section will be based upon, but not limited to, the degree to which the Vendor demonstrates direct experience with all aspects of performing security risk analysis and vulnerability testing in large, medium and small networked organizations, and broad expertise with this type of work. Importance is given to the specific project

role the Vendor has performed, as well as the scope and complexity of the projects in which the Vendor has participated. Both depth and breadth of experience are important.

RESPONSE – CONFIDENTIAL INFORMATION BELOW – NOT TO BE SHARED

Emagined Security has included at least five (5) representative projects that Emagined Security has performed for customers during the three (3) years preceding the Proposal due date. Emagined Security additionally has approximately a dozen additional references in Washington State including local government agencies, local cities and counties that would be willing to be references and can be released in a non-public document.

Ivanti

Project Statement: Emagined Security has performed penetration testing for the Ivanti Software Corporation. The Penetration testing includes web application penetration testing, Network Penetration Testing and configuration reviews to ensure that Ivanti Software Corporation is able to meet its various compliance requirements. It has additionally grown to incorporate new acquisitions added to their software portfolio. Emagined Security performs extensive project management to ensure knowledge transfer to the organization to ensure they understand the vulnerabilities identified during the testing. Emagined Security is additionally contacted to perform FedRAMP penetration testing and MSS Security Services to protect their environments from breaches.

Project's Deliverables: Emagined Security provides actionable assessment results highlighting areas of strength and areas for improvement. These deliverables include weekly, details status reports of potential vulnerabilities, Incidents and ticketing information. They also include penetration test reports, remediation results and 3rd party penetration testing reports for release to public entities.

Project's Duration: Penetration Testing incorporates several months of testing over the course of each year including up to 24 web applications and several thousand IPs. This project has been extended into multiple years and renewed for 2021.

Results: Emagined Security's reports have been used to reduce vulnerabilities and improve the overall security posture of the organization.

Nice InContact

Project Statement : Emagined Security has been performing formal penetration testing for Nice InContact for several years and is renewing for a Multi-year contract. Emagined Security has performed 2 of the global penetration tests incorporating applications, internal and external network infrastructures.

Project's Deliverables: Emagined Security provides actionable assessment results highlighting areas of strength and areas for improvement.

Project's Duration: Penetration Testing incorporates several months of testing over the course of each year including up to 20 web applications and several thousand IPs.

Results: Emagined Security's reports have been used to reduce vulnerabilities and improve the overall security posture of the organization.

NeoTech

Project Statement: Emagined Security performs ongoing Vulnerability assessments for NeoTech to assist in their CMMC requirements for the federal government. Emagined

Security additionally provides MSS Services to protect their environment from malicious intruders and provides Level 1 Incident Response services.

Project's Deliverables: Emagined Security provides actionable assessment results highlighting areas of strength and areas for improvement.

Project's Duration: Penetration Testing incorporates monthly reviews for vulnerabilities and is used to assess several thousand IPs.

Results: Emagined Security's reports have been used to reduce vulnerabilities and improve the overall security posture of the organization.

Community Hospital Corporation (CHC)

Project Statement: Emagined Security performs multiple application and infrastructure penetration tests at hospitals and infrastructures protected by CHC. This penetration testing is to assist in the protection of HIPAA data. Emagined Security also performs MSS Services for CHC Hospital and provides dashboards for Vulnerability Assessment Data in their MSS Dashboard data. Emagined Security also assists CHC with detailed Architecture and network support to enable their complexed VPN structures, multiple hospitals and outsourced vendors to securely communicate.

Project's Deliverables: Emagined Security provides actionable assessment results highlighting areas of strength and areas for improvement. Deliverables can include vulnerability assessment reports, penetration test reports, Firewall configuration and architecture design reviews, SOC service reports and network architecture design.

Project's Duration: Penetration Testing incorporates monthly reviews for vulnerabilities and is used to assess several thousand IPs. Additionally, a focused Penetration Test was used to review applications over a several month period. Projects at CHC have been ongoing for several years and continue to renew each year based on the professionalism and details put into these engagements by Emagined Security employees.

Results: Emagined Security's reports have been used to reduce vulnerabilities and improve the overall security posture of the organization.

Golden1 Credit Union

Project Statement: Emagined Security has performed Red Team and progressive penetration testing for Golden1 Credit Union for several years. Penetration Testing at Golden1 can incorporate Red Team testing, Web application penetration tests, network penetration tests, Wireless penetration tests, physical security assessments. Emagined Security additionally performs Phishing and Pharming attempts approved by the Auditor's Office as well as USB key drops and physical access to attempt full exploit and break-in of possible vulnerable systems.

Project's Deliverables: Emagined Security provides actionable assessment results highlighting areas of strength and areas for improvement.

Project's Duration: Penetration Testing and Red Teaming incorporates several custom tests twice a year to simulate actual attacks against the infrastructure. These tests are conducted over a several month period.

Results: Emagined Security's reports have been used to reduce vulnerabilities and improve the overall security posture of the organization.



REQUEST

Provide resumes (in Section V), which include information on the individuals' particular skills related to IT risk analysis and security testing, education, certifications experience, significant accomplishments and any other pertinent information.

RESPONSE

Resumes have been provided in Attachment 1: Section V. We would welcome having our Emagined Security staff to be interviewed by the State. Our current lead staffing for this project would consist of as needed. Additional staffing will be utilized to assist the senior staff as required by the engagement:

REQUEST

Demonstrate skills to communicate clearly, concisely and effectively both verbally and in writing.

RESPONSE

Emagined Security believes the best way to communicate is with our proven project management methodology. Emagined Security will assign an experienced project manager that enables the teams to communicate in both team meetings, emails and written documents (see our project methodology and project management approaches).

REQUEST

Describe the firm's methods for maintaining staff qualifications.

RESPONSE

All penetration testers' skills are being continually reevaluated

- All penetration testers are being required to acquire at least one additional certification per year to ensure skills are up to date
- During all training penetration tester are being challenged to continually identify ways to improve our methodology
- We are scheduling a new internal program of bi-weekly training to further enhance our skills
- An annual review process is being created to reassess skills each year

All work is completed by CISSP, CEH, OSWE and OSCP Certified engineers located in the United States.

- No testing or data is off-shored
- All employees are US Citizens
- All employees are background checked by the State of Washington Auditors office as well as pass Emagined Security's background check.
- No penetration testing is outsourced to 3rd parties.

REQUEST

Management approach, methodology and implementation strategies for managing and delivering their product.

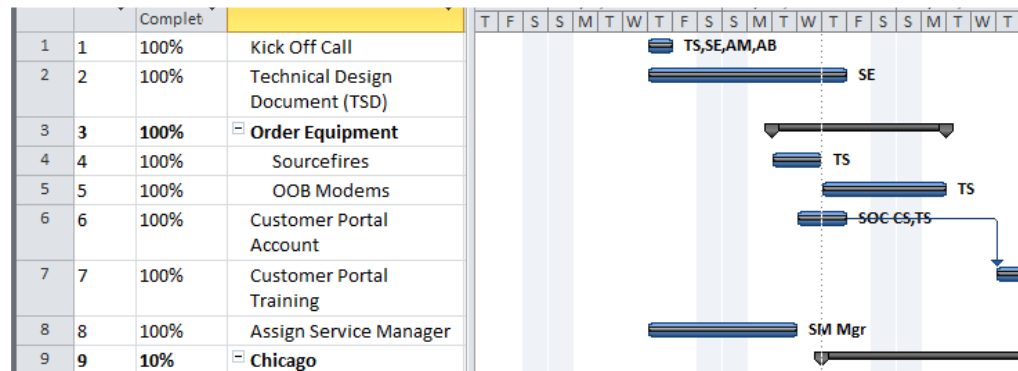
RESPONSE

Emagined Security utilizes a proven project management methodology that allows us to consistently monitor project status, budgets and quickly escalate and resolve issues. Emagined Security has performed similar engagement for other State agencies such as the State of Colorado.

At a minimum, we recommend that the following project management methods be established for the project.

High Level Project Plan:

The following high level project plan portrays the general approach and estimated milestones associated with our proposed approach.



Emagined Security has broken project management into two (2) types of engagement. Small Web application and infrastructure tests that are performed over a short period (Normally one – two weeks). And longer engagements that may span weeks to months.

Project Tracking and Status Reporting:

A detailed project plan will be developed at the beginning of the project. The plan will be reviewed and approved by the project sponsors. Progress will be monitored against the approved plan. Formal status reports will be delivered on a schedule defined by the project sponsor. The status report should include activities completed in the reporting period, activities not completed, a discussion of tasks and deliverables in each individual project activity to be completed in the following reporting period. Any issues that potentially bear on project success will be identified in this section. The status reports will be reviewed in regular project status meetings. The project sponsor will define the frequency of status reporting, but Emagined Security recommends that the status meetings be conducted on a weekly basis. The primary point of contact from Emagined Security will attend the status meetings.

Issues Management and Escalation:

Effective issue management is a critical success factor for the management of challenges that are experienced during the project life cycle and allows for the following:

- Visible decision-making process;
- Means for reaching consensus on questions concerning the project;
- Project key decision documentation.

An issues log will be maintained to log and track all issues. Open issues will be reviewed during project status meetings and escalated if needed to the executive project sponsor.

Scope Change Management:

A key to success in project management is the ability of the project manager and project team to effectively manage scope. When issues occur, either the requirements are not properly bounded or the scope is not controlled. There is a natural discovery process in all projects due to factors such as omissions, mistakes, creativity, misunderstandings, and

external influences. This discovery process normally creates pressure to expand scope. The purpose of a scope management process is to constructively manage that pressure.

Scope expansion is acceptable as long as:

- Both parties agree that the new requirements are justified;
- Impact to the project is analyzed and understood;
- Resulting changes to the project (e.g. cost, timing, quality, and human resources) are approved and properly implemented.

The main tool the project manager uses to manage scope is the Statement of Work (SOW) and recorded change requests. The SOW specifies the original agreement between the Customer and Emagined Security. Change requests are created to document any subsequent change to this baseline scope and are tracked by the project manager. Throughout the project, proposed changes are documented and screened by the project manager. The primary vehicle communicating potential scope issues is the weekly status report. The project manager determines which suggested changes might be necessary, and these are investigated to determine the impact of accepting or rejecting them. When the impact analysis is complete, the change is either approved and the project plan is adjusted to reflect the decision or the change is rejected. At any point in time, the current project scope is determined by the baseline scope defined in the SOW plus all the approved change requests.

Critical Success Factors:

Critical success factors assist all parties in ensuring the project's ultimate success. They include the following:

- An Executive Sponsor who actively supports the project and project team should be able to spend sufficient time on the project to stay abreast of any issues and the status of the engagement at any point in time.
- Efficient communications of work-in-process and gathered materials input into the project. We will establish a common repository of project-related data that will be maintained for the engagement team and this data will be a final deliverable of the engagement. The Project Sponsor will be notified of the value-added opportunities identified as a direct result of this engagement.
- Dedication to timely responses to requests from the consulting team.

At the highest level, we consider a project successful when the client agrees that the co-developed goals have been achieved. A few key aspects of ensuring and measuring success are:

- Co-developing goals and success criteria before the project begins.
- Continuous communication throughout the project to keep both parties abreast of progress and to obtain interim buy-in to work-in-process as it emerges.
- Customer satisfaction interview with the Project and Executive Sponsors at the end of the project to determine the level of satisfaction based on deliverables as compared to success criteria defined at the beginning of the project.

This approach is based on our belief that to obtain optimal results, it is essential to maintain feedback throughout the engagement.

Knowledge Transfer

At Emagined Security we practice Knowledge Transfer to better enable our clients to meet the challenges of securing business operations. Our experience shows that those

clients who are best informed are better clients because they quickly grasp the impact of our analysis and the fact that we are working with their best interest in mind. Through knowledge transfer, our clients become stronger, better informed and more responsive to the results of Emagined Security's analysis and support.

REQUEST

Describe their ability and capacity for delivering services proposed.

RESPONSE

Emagined Security has several project and program managers that work to schedule penetration tests efficiently and coordinated to ensure that Customers have penetration tests scheduled in a timely manner.

Emagined Security core service is providing penetration testing, vulnerability assessments and risk assessments. All consultants are familiar with our proposed methodologies and have performed these services for numerous customers over the course of Emagined Security's approximately 19 years.

Emagined Security has over 40 Consultants with extensive information security backgrounds. Of those 40 consultants, 25 have capabilities to perform penetration testing. All are background checked, US based including several with extensive state and local government experience. Emagined Security understands how to work with smaller government agencies and how to not overwhelm responses to penetration test reports to overwhelm those agencies.

All current penetration testers have been background checked as well by the Washington State Patrol and have background checks on file with the SAO office.

As demonstrated in our detailed methodologies detailed above, Emagined Security has the proven methodologies, the skills and the experience to provide the services which have been proposed. If additional details are requested, a Teams Meeting can be setup to demonstrate our abilities / capacity.

REQUEST

Sample report (Scored) Note: report should be cleansed of confidential information.

RESPONSE

Sample report is included in Attachment 2.

SECTION III-a – QUALIFICATIONS SECTION (Optional and separate from Section III)

REQUEST

As a separate part of the response to this section we are interested to hear the consultant's perspective on what risks the potential contractor cannot control in this project.

Additionally, we would like the consultant's perspective on services that would add value to our proposed scope of work, but that we did not request.

RESPONSE

Risks: Emagined Security can control many factors of a penetration test. We review all our tool configurations to ensure there are no destructive tests run. We also control our

time and penetration testing functions to ensure our schedules are able to be fixed. Unfortunately, we cannot control the schedules on the client side. Most issues that arise during a test have to do with clients not being prepared or provided access and necessary information when needed. Clients that do not identify in place security controls, Web application firewalls, Internal firewalls, Honeypots, etc. can slow down a penetration test or provide results that are not properly represented.

Consultant Perspectives on Services Adding Value: Emagined Security has a variety of services that enable the clients to better understand and manage issues identified during testing. This includes extensive knowledge transfer & training and cooperative working teams most at no additional charge.

Knowledge Transfer & Training: We believe that knowledge transfer and training can provide to the Washington State Auditor's office, better products. As a team we can facilitate real improvements and help protect the State of Washington, its agencies and local governments.

Cooperative Working Teams: Emagined Security believes the better cooperation we have between Emagined Security and the Washington State Auditor's Office, the more benefit will be obtained from the work performed. This can be demonstrated by previous working relationships with the Washington State Auditor's Office and our ability to streamline processes as testing continued and our ability to accommodate the changing requirements for work to be performed.

Additionally, by having a cooperative working team, we can lower future costs and assist the Washington State Auditor's office in facilitating a "Best in the nation" Vulnerability Management Program.

OSINT- Open Source Intelligence: Emagined Security can provide open-source intelligence gathering on potential entities and agencies that does not directly engage these entities. This open-source intelligence can be utilized to better scope an external engagement with an entity or agency as well as provide a general security posture. Emagined Security recommends OSINT be performed at the beginning of every penetration test scoping engagement to provide additional information about the agency or entity being tested to ensure a comprehensive view is placed on what an attacker might review before attacking one of these organizations.

Threat Hunting: Emagined Security can identify, preserve, analyze, and review electronic evidence during a penetration test. As such, Emagined Security can use tools that are available to identify if systems have been penetrated.



EMAGINED SECURITY

SECTION IV – CUSTOMER REFERENCES (MR)(PASS/FAIL)

SECTION V – RESUMES (MR) (SCORED)

REQUEST

The proposer must provide resumes for key staff and include information on the individual's specific skills, experience, certifications significant accomplishments and responsibilities assumed on other similar projects related to the services proposed.

RESPONSE

Emagined Security maintains an elite team of over 40 consultants currently engaged with existing clients. Averaging over 15 years of security experience, consultants include highly technical individuals, project managers and former Information Security Executives. Various diverse backgrounds include former Fortune 100, C-level, Big Four Accounting firms, strategy consultants, process engineers, etc., with years of security experience. Team members would be selected based on the respective knowledge, skills and attributes associated with each of the project tasks, however, the project will be managed by the practice leads that follow.

<Resumes have been provided in Attachment 1: Section V>

Additional resumes of other staff that can assist are available if required. The team will enable the ability to lead multiple engagements at the same time and give the Washington State Auditor's office the ability to streamline the process of performing these penetration tests.

SECTION VI – CERTIFICATIONS AND ASSURANCES (MR)(PASS/FAIL)

REQUEST

Section VI must include a signed Certifications and Assurances form, see: Exhibit A - Certifications and Assurances (MR)

RESPONSE

K646-RFQQ-2011

EXHIBIT A – CERTIFICATIONS AND ASSURANCES

I/we make the following certifications and assurances as a required element of the proposal to which it is attached, understanding that the truthfulness of the facts affirmed here and the continuing compliance with these requirements are conditions precedent to the award or continuation of the related contract(s):

1. I/we declare that all answers and statements made in the proposal are true and correct.
2. I/we certify that non-audit services have not been performed on behalf of state agencies or local governments in Washington State (see <http://www.gao.gov/govaud/iv2011gagas.pdf>) at any time during the previous four years by our firm or by any individual relative to this proposal.

Or

I/we are disclosing that non-audit services have been performed during the previous four years by our firm on behalf of state agencies or local governments in Washington State. I/we understand that additional assurances will be required related to the nature of the non-audit services provided to state agencies or local governments selected for inclusion in the audit to certify that I/we meet Government Auditing Standards 2018, General Standards for Independence.

Date	Audited Entity	Describe non-audit services provided	Audited entity contact
9 FEB 2021	3 LOCAL	SEC. MONITORING	PEG BODIN

GOVERNMENT ENTITIES


3. The contractor warrants that all persons performing work under this contract and any subcontracts are free from personal and external impairments to independence.
4. The prices and/or cost data have been determined independently, without consultation, communication, or agreement with others for the purpose of restricting competition. However, I/we may freely join with other persons or organizations for the purpose of presenting a single proposal.
5. The attached proposal is a firm offer for a period of 60 days following receipt, and it may be accepted by the State Auditor's Office without further negotiation (except where obviously required by lack of certainty in key terms) at any time within the 60-day period.
6. The project staff and subcontractors identified in Section III – Staffing will be assigned for the duration of the project. We agree that no substitutions or deletions of project personnel will occur without first requesting and the receiving approval, in writing, from the State Auditor's Office.
7. In preparing this proposal, I/we have not been assisted by any current or former employee of the State of Washington, or any current or former employee of a local government in the State of Washington, whose duties relate (or did relate) to this proposal or prospective contract, and who was assisting in other than his or her official, public capacity. Neither does such a person nor any member of his or her immediate family have any financial interest in the outcome of this proposal. (Any exceptions to these assurances are described in full detail on a separate page and attached to this document.)
8. I/we understand that the State Auditor's Office will not reimburse me/us for any costs incurred in the preparation of this proposal. All proposals become the property of the State Auditor's Office, and I/we claim no proprietary right to the ideas, writings, items, or samples, unless so stated in this proposal.
9. Unless otherwise required by law, the prices and/or cost data which have been submitted have not been knowingly disclosed by the proposer and will not knowingly be disclosed by him/her prior to submission, directly or indirectly to any other proposer or to any competitor.
10. I/we agree that submission of the attached proposal constitutes acceptance of the solicitation contents and the attached Special Terms and Conditions, and General Terms and Conditions. If there are any necessary exceptions to these terms, I/we have described those exceptions in detail on a page attached to this document.

11. No attempt has been made or will be made by the proposer to induce any other person or firm to submit or not to submit a proposal for the purpose of restricting competition.
12. I/we grant the State Auditor's Office the right to contact references and others, who may have pertinent information regarding the proposer's prior experience and ability to perform the services contemplated in this procurement.
13. Bidder Responsibility Criteria; Bidder certifies that Bidder has not, within the three-year period immediately preceding the date of release of this competitive solicitation, been determined by a final and binding citation and notice of assessment issued by the state of Washington Department of Labor and Industries or through a civil judgment to have willfully violated state minimum wage laws (RCW 49.48.082; Chapters 49.46 RCW, 49.48 RCW, or 49.52 RCW). Bidder attests under penalty of perjury that the foregoing statement is true and correct.
14. I/we identify the following firm principals as participants in the Washington State 2008 Early Retirement Factor Program...

PARTICIPANTS

☒ NO PARTICIPANTS

On behalf of the firm submitting this proposal, my name below attests to the accuracy of the above statements.


CEO
17 FEB 2021

Signature of Proposer
 Title
Date



SECTION VII – REPORT SAMPLES (MR)(PASS/FAIL)

REQUEST

The proposer must provide one sample report that discusses work, and its related results, in areas similar to those that are referenced in the first set of bulleted items in Section III above.

This sample report may either be an actual report that the proposer has delivered to a previous client, as long as the contents have been redacted according to any applicable laws, regulations, or agreements with that client, or it may be a mock report that the proposer has generated specifically for their response to this RFQQ.

This sample report will be scored based on how well its components respond to items listed under item “d.” under “Report Results” on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.

RESPONSE

Emagined Security reports contain the following vital information. **A full sample reports is in Attachment 2.**

Emagined Security will prepare a consolidated report of our findings for Washington State Auditor. This report template will be created and updated with the direction of the Washington State Auditors guidance and can be updated based on the State’s needs. The report will be delivered first in draft form so as to allow time for the Washington State Auditor to prepare a response. Upon receipt of the response from the Washington State Auditor, Emagined Security will prepare a final report, which will incorporate responses.

Reporting is broken down in sections based on the applications so that portions of the report can easily be separated allowing the least privilege of information to be shared with individuals that are working on remediation of the findings. These reports 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.

Additionally, Emagined Security breaks down the identified vulnerabilities into a vulnerability class dispersion pie chart enabling your company to determine from the identified findings any trending on the types of vulnerabilities identified during the penetration testing.

Overview of the Engagement

The section will include the objectives and an overview of the engagement including description of the tasks performed by Emagined Security.

Engagement Plan / Scope

The section will include the scope of the engagement including services performed, the engagement plan, in scope and not in scope, as well as the scope of systems the testing is performed against.

Summary of Findings

The section will include a summary of the vulnerabilities identified during the course of the penetration test and will also provide a location for easily identified remediation results. As a note, all vulnerabilities identified and reported by Emagined Security are manually verified to ensure no reporting of false positives. Emagined Security will also provide feedback on areas where exceptional security controls have been identified.

Testing Methodology

A high-level description of Emagined Security's methodology used for performing the assessment will be documented in this area.

Tools

This section will provide a list of tools used during the specific penetration testing engagement.

Identified Vulnerabilities, Risks & Recommendations

A separate section for each of the task(s) will be devoted to the findings discovered in that task. Each section will provide detailed information as to the issue of concern and a possible remediation or resolution to the problem. These sections will, as appropriate, have a technical focus.

Severity Level Descriptions

Each vulnerability or risk identified is labeled with a severity (Risk) factor, as follows:

Emergency: Findings with this level can be used to breach the integrity of a company system. This level of risk is the most serious as it relates to an actual or imminent breach in security.

High Risks: Findings with this level of risk are serious deficiencies that have already, can or most likely will result in serious breaches in the hosting infrastructure ability to maintain its security posture.

Medium Risks: Findings at this level of severity could have a moderate impact to the organization if an attack were successful.

Low Risks: Findings at this level of severity allow an attacker to gain knowledge of the organization.

Informational: Findings with this level of severity are harder to quantify but are still security issues and are recommended to be remediated by the next major release.

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

Ease of Exploit

Easy: A finding that can be easily exploited by commonly available tools on the Internet, well-known exploits, and/or were little to no technical expertise is required.

Medium: Findings that require a medium level of effort 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 a detailed technical expertise is required.

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

Conclusions and Recommendations

This area details Emagined Security's overall conclusions and recommendations based upon the issues found during the assessment. In addition, the section provides a more strategic, long-term focused view to combat the weaknesses discovered by Emagined Security.



SECTION VIII –SECURITY QUESTIONNAIRE (MR)(PASS/FAIL)

REQUEST

The proposer must provide a completed State Auditor's Office (SAO) Data Sharing Questionnaire (see Exhibit E). If selected the vendor may be asked to provide verification of responses provided to the questionnaire which may include: security audits such as a SOC 2 report or any IT security reviews completed by an external auditor; additional questions; onsite verification.

RESPONSE

EXHIBIT E: STATE AUDITOR'S OFFICE (SAO) SECURITY QUESTIONNAIRE

Please answer with as much description and detail as possible to the following questions. Questions and requests for information are in support of SAO compliance requirements derived from OCIO Standard No. 141.10. This standard can be retrieved from: <https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets>.

Physical and Environmental Protection

1. Please describe the physical attributes and controls used to protect computer hardware, documents and all related material that could or will be associated with any contracted data exchange between the State Auditors Office and the audited entity.

[Emagined Security stores project data in an encrypted system within a locked cage with cameras recording all access. The Network is segregated into a production network separated from all corporate and DMZ networks with limited access by authorized personnel. Documents, if printed are kept in locked offices or destroyed when they become obsolete to the needs of Emagined Security. Any systems in a cloud environment are locked to IP addresses for access and do not allow general internet access]

2. Will your organization be storing any contract related data on other systems in addition to workstations such as servers or cloud service providers? If so, describe the physical security and controls in order to protect contract related data.

[yes, Emagined Security utilizes similar technologies to SAO with regards to Microsoft Office 365 and Teams, Emagined Security has Office 365 2-Factor Authorization on all employees and locks all files to the least privilege methods]

3. Will your organization's assigned agents associated with any contract with SAO be accessing and storing any contract data on mobile devices such as phones and tablets. If so, describe any controls used to protect contract related data on those devices.

[No]

Network Security (Regarding any systems that will be storing, processing or used for transitory (email for example) functions with contract related data)

1. If applicable, how will your organization apply and enforce network controls to protect segments and individual systems with each segment in order to prevent unauthorized access to contract related data.

[Emagined Security uses 2 factor authorization via a VPN to access systems remotely, only authorized individuals are able to access the network, all systems log access (both system and VPN)]

2. How does your organization ensure that systems are up-to-date with latest software security patches and updates? Please explain your organization's patch management process and provide your organization's patch management policy.

[Where able, Emagined Security patch management is automated via the Microsoft Automatic updates, additional patches are applied when notified via Emagined MSS Services SOC (about the Emagined Security software configurations) and applied.]

3. Please provide your organization's password policy.

Emagined Security Policy Statement - [Emagined Security relies heavily on 2 factor authorization and not necessarily password protection, Emagined Security requires individuals to change their password every 90 days, password complexity is extensive, requiring passwords to be a minimum of 10 characters in length, contain upper, lower characters, a number and special character and be hashed and checked against a database of 1.3 billion compromised passwords.]

Operations Management

1. Describe your organizations media handling and disposal process? Please provide your associated policy if applicable.

Emagined Security Policy Statement - [All disposable media is destroyed via shredding, hard drives are DOD wiped with Emagined Security forensic equipment.]

2. Does your organization have a data backup processes in place that will capture and backup any data related to the contract? If so, please describe the backup process and procedures and any controls (e.g., encryption) used to protect contract related data in backup systems? Please provide your associated policy if applicable.

Emagined Security Policy Statement - [Currently Emagined Security has backup procedures for all Emagined owned and operated servers and workstation systems. Systems are backed up daily to a segregated storage, only used for backup purposes with only authorized administrators having access]

Security Monitoring and logging

1. What type of auditing capabilities, features and settings does your organization enable on systems such as security event logs? Please provide your organization's policy associated to this question.

[Emagined Security runs a Security Operations Center to review logs and alerts. For example, multiple unauthorized access attempts, when identified, trigger emails to an administrator that checks system access and login attempts to validate there are no malicious activity on the systems. No

systems have internet access or ability to access the internet that will be used from the State of Washington]

2. How long are logs retained on any system that will be handling contract related data?

[Minimum of 90 days]

Incident Response - In the event of any confirmed compromised or breach of data related to protected contract related data, explain or provide your organization's Incident Response protocol or plan? Please provide all associated organizational policies with this question.

Emagined Security Policy Statement - [Emagined Security has a full incident response handbook that details how individual breaches are handled, Emagined Security is a leader in Incident Response handling procedures. Additionally, if an Emagined Security system is compromised, any client with data on that system would be notified individually with details of what data was compromised. All data is encrypted so any compromise of data would be a complicated attack.

Emagined Security can provide Specific full policies if we are the winning bidder. Since this is a publically releasable document, Emagined Security cannot provide our specific policies since they are confidential.]

Data Security – 1) Please explain any controls (encryption; role-based security for example) your organization uses to protect contract related data on systems such as servers to prevent unauthorized access to data-at-rest.

Emagined Security Encryption - Emagined Security has a separate workspace for State of Washington data, enabling us to properly encrypt State data segregated from all other client data at Emagined Security. All State data that is at rest at Emagined Security is encrypted when at rest and in transit. All SAO data is additionally locked to the least privilege method of data protection.

2) Will your organization be using any system(s) for data transfer or transmission such as file transfer or email type systems to transmit contract related data? If so, please describe all controls that will ensure the data exchange is secure and that data cannot be deciphered during transmission.

Emagined Security Data Transfer – Emagined Security utilizes a Microsoft office 365 encryption so that no unencrypted sensitive data is transmitted to State Employee email addresses. This is to help protect the state employee from having data in an unencrypted fashion on their computer or email system; making is susceptible to unnecessary disclosure.

SECTION IX – CONFIDENTIALITY AND NONDISCLOSURE AGREEMENT, (MR)(PASS/FAIL)

REQUEST

The proposer must provide a completed State Auditor's Office (SAO) Confidentiality and Nondisclosure agreement (see Exhibit F). Signed NDA

RESPONSE

K646-RFQQ-2011

EXHIBIT F – CONFIDENTIALITY AND NONDISCLOSURE AGREEMENT

CONFIDENTIALITY AND NONDISCLOSURE AGREEMENT

This Confidential and Nondisclosure Agreement ("Agreement") is entered into by and between the State Auditor's Office, an agency of Washington State government ("SAO"), and ("Recipient").

Recipient acknowledges that SAO has certain confidential or sensitive information and/or material. Recipient requires access to this information or material to complete the IT Security Audit. SAO agrees to release this information to Recipient for those purposes pursuant to the terms and conditions contained in this Agreement. Recipient agrees to the terms and conditions herein.

NOW THEREFORE, in consideration of the above premises and the promises contained herein, the parties agree as follows:

1. Whenever used in this Agreement, the term "Confidential Information" will mean (i) information exempt from disclosure to the public or other unauthorized persons under either chapter 42.56 RCW or other state or federal statutes, unless otherwise identified as non-confidential at the time of disclosure; or (ii) any other information which SAO has identified to Recipient in writing as confidential at the time of disclosure or within thirty (30) days after disclosure; or (iii) information which would ordinarily be considered confidential or proprietary in the light of the circumstances surrounding disclosure. Confidential Information may take the form of (but is not limited to) plans, calculations, charts, concepts, know-how, inventions, licensed technology, design sheets, design data, diagrams, system design, materials, hardware, manuals, drawings, processes, schematics, specifications, instructions, explanations, research, test procedures and results, equipment, identity and descriptions of components or materials used, social security numbers, protected health information, personally identifiable information, IT security test results or any other material or information supplied by or on behalf of SAO, or that is disclosed to or becomes known by Recipient as a result of its dealings with SAO. Confidential Information may be in tangible or intangible form. SAO's failure to expressly identify Confidential Information as such shall not in any way lessen or negate Recipient's obligation to keep such information confidential in accordance with this Agreement.
2. Notwithstanding the foregoing, the term "Confidential Information", shall not be construed to include information that (i) is or becomes readily available in public records or documents, other than as a result of a disclosure by Recipient or other entity acting on behalf of Recipient, or (ii) which can be documented to have been known by Recipient prior to its disclosure by SAO, or (iii) which is disclosed pursuant to applicable law, judicial action or government regulations, including without limitation the Washington State Public Records Act, RCW 42.56, et seq.
3. The Recipient acknowledges that the Confidential Information is confidential and proprietary information of State of Washington (SOW) and local governments and that its protection is essential to the security and mission of SOW and local governments. The purpose of this agreement is to enable SAO to make disclosure of the Confidential Information to the Recipient while still maintaining rights in and control over the Confidential Information. The purpose is also to preserve confidentiality of the Confidential Information and to prevent is unauthorized disclosure. It is understood that this agreement does not grant Recipient an express or implied license or an option on a license, or any other rights to or interests in the Confidential Information.
4. The Recipient shall, and require its employees, officers, independent contractors, and subcontractors, and any other entities acting on its behalf (collectively "Affiliates") to:
 - (a) copy, reproduce or use Confidential Information only for the purpose described herein and not for any other purpose unless specifically authorized to do so in writing by SAO; and
 - (b) not permit any other person to use or disclose the Confidential Information for any purpose other than those expressly authorized by this Agreement; and
 - (c) disclose such Confidential Information only to those of its Affiliates who require knowledge of the same for the purpose described herein; provided such Affiliates are obligated to maintain the confidentiality of the Confidential Information and otherwise comply with the terms of this Agreement; and
 - (d) implement physical, electronic and managerial safeguards to prevent unauthorized access to or use of Confidential Information, including without limitation, providing Affiliates a copy of the terms of this

57

K646-RFQQ-2011

Agreement. Such restrictions will be at least as stringent as those applied by the Recipient to its own most valuable confidential and proprietary information.

5. The acts or omissions of Recipient's Affiliates with respect to the Confidential Information shall be deemed to be acts or omissions of Recipient.
6. Recipient will not remove, obscure or alter any confidentiality or trade secret notation from the Confidential Information without SAO's prior written authorization.
7. Confidential Information will remain the exclusive property of SAO; upon completion of the project described in Section 1, or whenever requested by SAO, Recipient will promptly destroy or return to SAO all Confidential Information and all copies thereof, including summaries, reports or notes based thereon, unless otherwise expressly authorized by SAO in writing.
8. Recipient agrees that the breach of the terms of this Agreement would cause irreparable damage to SOW and/or local governments and their citizens. Therefore, Recipient agrees that if it should breach its obligations hereunder, Recipient will defend, indemnify, and hold SAO harmless from actual damages from losses that result from its breach, including the notification requirements of RCW 42.56.590. This includes attorneys' fees and costs of suit. Also, SAO has the right to seek an order to restrain Recipient from breaching this agreement. If SAO does seek such an order, Recipient agrees at this time to waive any claim or defense that SAO has an adequate remedy at law or in damages.
9. This Agreement will be construed and enforced in all respects in accordance with the laws of the State of Washington. The parties consent to the exclusive jurisdiction of the Superior Court of the State of Washington and exclusive venue in Thurston County, Washington.
10. Term. The Term of this Agreement shall be three years from the date of the last signature, provided however, the obligations of confidentiality shall continue and survive this Agreement.

APPROVED
State of Washington
State Auditor's Office

Signature

Print or Type Name

Title

Date

APPROVED

Recipient: EMAGINED SECURITY, INC.

Signature

Print or Type Name

Title

Date

Address

Phone



EMAGINED SECURITY

SECTION X – PROCUREMENT EVALUATION FOR EXECUTIVE ORDER 18-03 CERTIFICATION FORM (MR) (Scored)

REQUEST

Pursuant to RCW 39.26.160(3) (best value criteria) and consistent with Executive Order 18-03 –Supporting Workers' Rights to Effectively Address Workplace Violations (dated June 12, 2018), Office of the Washington State Auditor will evaluate bids for best value and provide a bid preference in the of 5 points to any bidder who certifies, pursuant to the certification attached as Exhibit G – Contract Certification for Executive Order 18-03 – Worker's Rights, that their firm does NOT require its employees, as a condition of employment, to sign or agree to mandatory individual arbitration clauses or class or collective action waiver.

RESPONSE

EXHIBIT G – PROCUREMENT EVALUATION FOR EXECUTIVE ORDER 18-03 CERTIFICATION FORM

CONTRACTOR CERTIFICATION EXECUTIVE ORDER 18-03 – WORKERS' RIGHTS WASHINGTON STATE GOODS & SERVICES CONTRACTS

Pursuant to the Washington State Governor's Executive Order 18-03 (dated June 12, 2018), the Office of the Washington State Auditor's Office is seeking to contract with qualified entities and business owners who certify that their employees are not, as a condition of employment, subject to mandatory individual arbitration clauses and class or collective action waivers.

Solicitation No. K646 RFQQ 2011

I hereby certify, on behalf of the firm identified below, as follows (check one):

☒ **NO MANDATORY INDIVIDUAL ARBITRATION CLAUSES AND CLASS OR COLLECTIVE ACTION WAIVERS FOR EMPLOYEES.** This firm does NOT require its employees, as a condition of employment, to sign or agree to mandatory individual arbitration clauses or class or collective action waivers.

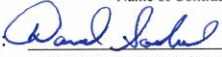
OR

☐ **MANDATORY INDIVIDUAL ARBITRATION CLAUSES AND CLASS OR COLLECTIVE ACTION WAIVERS FOR EMPLOYEES.** This firm requires its employees, as a condition of employment, to sign or agree to mandatory individual arbitration clauses or class or collective action waivers.

I hereby certify, under penalty of perjury under the laws of the State of Washington, that the certifications herein are true and correct and that I am authorized to make these certifications on behalf of the firm listed herein.

FIRM NAME: EMAGINED SECURITY, INC.

Name of Contractor/Bidder – Print full legal entity name of firm

By: 
Signature of authorized person

DAVID SOCKOC
Print name of person make certifications of firm

Title: CEO
Title of person signing certificate

Place: SAN CARLOS CA
Print City and state where signed

Date: 17 FEB 2021

ATTACHMENT 1: Section V – Resumes

<This Page Intentionally Left Blank>

Emagined Security Penetration Test Team

Produced by:
Paul Underwood
[Emagined Security](#)
801.294.2917
paul@emagined.com



Main Website: www.emagined.com
Security Dashboard: dashboard.emagined.com
Security Blogs: blog.emagined.com

Introduction

Emagined Security, a privately owned and operated company, has been helping organizations with their security needs with an excellent track record of success since 2002. The company is comprised of 40 senior information security professionals in the industry, with an average of 15+ years of experience. Consultants have varied and diverse backgrounds in information security with high levels of knowledge, industry certifications and practical experience. Various diverse backgrounds include former Fortune 100, C-level, Big Four Accounting firms, strategy consultants, process engineers, etc., with years of security experience. Team members would be selected based on the respective knowledge, skills and attributes associated with each of the project tasks, however, the project will be managed by the practice leads that follow.

Emagined Security was created to offer corporations a comprehensive array of sophisticated, adaptive security solutions that include both consulting and managed services. In support of this initiative, Emagined Security has built a highly talented organization specializing in information security consulting. The Company focuses on securing business solutions by providing a full complement of proactive, real-time, reactive, executive advisory, license advisory and support security services to global institutions, major corporations, and other smaller organizations, while providing a fully business-driven approach.

Emagined Security is the leading professional services provider for Information Security & Compliance solutions. Emagined Security empowers its clients to help them effectively manage IT risk in today's dynamic business environment. With deep industry and domain expertise, a proven track record, and by employing well known and respected individuals from the Information Security community, Emagined Security can scale quickly and efficiently to provide clients with the rapid response required by best-in-class organizations. Emagined Security's commercial clients cover a wide range of U.S. and global Fortune 500 organizations, including the financial services, energy, healthcare, high tech, manufacturing, & insurance industries.



EMAGINED SECURITY

Certifications

Emagined Security ethical hackers possess a variety of certifications including but not limited to Certified Information Systems Security Professional (CISSP), C|EH, InfraGard, Offensive Security PWB (**OSCP**), Thales nCSE, A++ Certification, Systems Security Certified Professional, Certified Computer Examiner, EnCase Certified Examiner, A+ Certified Service Technician, Server+ Certified, HP Accredited Platform Specialist – Proliant (APS), Microsoft Certified Professional Systems Engineer (MCSE), Certified in Homeland Security – Level 3 (CHS-III)*, GIAC Certified Firewall Analyst (GCFW)*, GIAC Security Essentials Certification (GSEC)*, Cellebrite UFED Certified – Mobile Devices (C00028), Cellebrite UFED Physical Certified – Mobile Devices (P00169), Securing Solaris – The Gold Standard (GGSC), Katana Forensics Lantern iOS First Responder Certification, Katana Forensics Laboratory iOS/Mac OS X Certification, **GIAC**, Certified Forensic Analyst (GCFA) 2014, DoD Clearances, Cisco Certified Networking Professional Security Specialist 1, Cisco Certified Networking Professional + Security (CCNP + Security), Check Point Certified Security Administrator (CCSA), Cisco Certified Networking Professional (CCNP), Cisco Certified Network Associate (CCNA), Microsoft – Microsoft Certified Professional, Systems Engineer, & Trainer, Novell – Certified Novell Administrator, Engineer, & Instructor, Project Management Institute – Project Management Professional, International Information Systems Security Certification Consortium (ISC)², ES – Enterasys Dragon Certification, State of California Peace Officer Standards and Training (P.O.S.T.) Level II, Member High Technology Crime Investigation Association (H.T.C.I.A.)



Areas of Expertise

*Ethical Hacking /
Penetration Testing*

*Vulnerability
Management*

*Vulnerability
Assessments*

Digital Forensics

*Fraud Detection /
Prevention / Control*

*Network Architecture
Analysis / Design*

*Security / Risk
Assessment*

*Process Development /
Instantiation*

*Network, Application and
Perimeter Security*

*Problem Solving –
Concrete & Abstract*

Analytics and Research

*Program Creation,
Management and
Development*

Documentation

*Converged Environments
/ Cloud*

Social Engineering

*Law Enforcement
Relations and
Collaboration*

Patrick Cleary, Executive Consultant

Patrick Cleary is a executive security consultant with Emagined Security, providing expertise in the fields of Ethical Hacking/Penetration Testing, Digital Forensics and Risk/Fraud Protection. Prior to joining Emagined Security, Mr. Cleary served in both technical and managerial capacities at Visa Inc., Fairchild Semiconductor and KHQ-TV. Mr. Cleary is a versatile communicator and innovator, with demonstrated ability to translate complex security issues and challenges into proven, viable security control measures/results as implemented throughout all levels of an organization. Given Mr. Cleary's diverse background and experience in enterprise environments, he is uniquely positioned to blend security and business advocacy into cohesive enterprise solutions with a high level of efficacy.

Key accomplishments:

- Author of over twenty keystone policy and procedural documents including the incident response and computer security team handbook, the perimeter security handbook and the computer forensics procedural guidelines documents. A vast number of the documents written by Cleary are still in use today.
- Lead assessor for more than fifty security assessments that required documented risk analysis, mitigation and containment research and controls evaluation and recommendation. Cleary worked across all facets of the organization to ensure security controls were understood, documented and implemented properly in accordance to recommendation and compliance.
- Lead tester on numerous penetration testing engagements, including a social engineering exercise complete with pivot and advancement protocols and behavioral pattern analysis, as well as coordinator and program lead for annual global security assessment efforts which conducted network penetration testing at a macro-level on both external and internal enterprise assets totaling in excess of 6500 systems and applications.
- Selected by the CISO of a Fortune 500 company to create, develop, socialize and lead a next-generation perimeter security program with core focus on the extensible perimeter, including cloud, converged and mobile platforms.
- Cleary oversaw the procurement, deployment and operations turn-over effort for a Fortune 500 company's web



EMAGINED SECURITY

Certifications

*CISSP, EnCE, CCE, APS,
MCSE, SSCP, A+*

*UFED Physical and
Logical Certified*

Affiliations

HTCIA

N-TEC

NCFTA

InfraGard

Education

*Eastern Washington
University (MFA)*

*University of Maine at
Farmington (BA)*

application firewall adoption. Through Cleary's direct involvement and program management, the organization was able to realize the successful instantiation and network incorporation of more than twenty web application gateways in a nine month interval.

- Cleary was the innovator and early adopter of a Fortune 500 company's cyber security program. Cleary established controls and programs to protect the organization from phishing, fraud, malware and similar nefarious activities as well as secured key partnerships with service leaders and innovators. The work undertaken by Cleary in this space is still being advanced today.
- Cleary has been the lead investigator or lead forensics consultant on over seventy five investigations, some of them extremely high-profile and news worthy. Cleary has contributed directly to these investigations by discovery of evidence and indicators of compromise that have been shared with law enforcement organizations including the United States Secret Service and Federal Bureau of Investigation. Cleary remains a staunch supporter of collaboration, knowledge-sharing and partnership with the men and women of law enforcement while ensuring organizations maintain their privacy.
- Cleary has been highly-praised and lauded for his contributions to information security at each organization where he has worked or interfaced. Cleary continues to bring daily passion, confidence and positivity to his work and ensures that every Emagined Security client leaves more secure and aware than before they engaged Emagined!



EMAGINED SECURITY

Areas of Expertise

*Ethical Hacking /
Penetration Testing*

Vulnerability Management

Vulnerability Assessments

*Network Architecture
Analysis / Design*

Security / Risk Assessment

*Process Development /
Instantiation*

*Network, Application and
Perimeter Security*

*Secure Software
Development*

*Web Application
Programming*

*Problem Solving –
Concrete & Abstract*

Analytics and Research

*Program Creation,
Management and
Development*

Documentation

*Converged Environments /
Cloud*

Social Engineering

Ramcés Chirino, Executive Consultant

Ramcés Chirino is a executive security consultant with Emagined Security, providing expertise in the fields of Ethical Hacking/Penetration Testing, Network Architecture, Software Development, and Program Management. Prior to joining Emagined Security, Mr. Chirino served in both technical and managerial capacities at Visa Inc. and the United States Navy. Mr. Chirino possesses strong skills in identifying client needs and fostering collaboration with multiple teams to formulate solutions. He has effective written and verbal communication skills in English, Spanish, and Portuguese, with demonstrated ability to bridge the gap between technical and non-technical personnel.

Key accomplishments:

- Implemented 3rd party security testing program for a Fortune 500 company, including formulating business justification, authoring request for proposals (RFP) and process documentation, performing cost savings analyses, and training personnel.
- Updated antiquated client processes to meet their respective requirements. The processes included moving from static documentation to database-driven applications to intelligently gather and manipulate data throughout the process lifecycle. Technologies used to implement these solutions included Windows SharePoint Services, OpenText Livelink, and custom programs.
- Developed a security management application to compose, generate, and track vulnerability assessments for a Fortune 500 company, which resulted decreased reporting times, multi-team collaboration, and a cost-savings of over \$1.5M to the company. Alongside the application was the implementation of programming best practices, including continuous integration and robust bug tracking for progressive development.
- Lead assessor for more than a hundred security assessments that required documented risk analysis, mitigation and containment research and controls evaluation and recommendation. Mr. Chirino worked across all facets of the organization to ensure security controls were understood, documented and implemented properly in accordance to recommendation and compliance.
- Lead tester on numerous penetration testing engagements, including a social engineering exercise complete with pivot and



EMAGINED SECURITY

Certifications

*GSEC, Security+, Oracle
Certified Professional Java
Programmer, CIW Perl,
JavaScript, Database
Specialist, and Web
Development Professional,
Project+, Network+, A+*

SSBI Top Secret Clearance

Education

*Western Governors
University (BS CIS)*

advancement protocols and behavioral pattern analysis, as well as coordinator and program lead for annual global security assessment efforts which conducted network penetration testing at a macro-level on both external and internal enterprise assets totaling in excess of 6500 systems and applications.

- Pioneered the implementation and integration of several technologies for a Fortune 500 company, which resulted in enterprise-wide adoption, including virtualization, full disk encryption, and configuration management. Received several awards in recognition of these achievements.
- Received a Navy and Marine Corps Achievement Medal (NAM) for working aggressively with Fleet Information Warfare Center to identify and eradicate network vulnerabilities, and successfully implement a shipboard information security program continue such practices.



Areas of Expertise

Ethical Hacking

*Information Technology,
Security Methodology*

Penetration Testing

Security Management

Problem Solving

*Project and Program
Management*

Embedded Controllers

*Secure SDLC
Development*

*Software Development
(Agile / Waterfall)*

*Vulnerability
Assessments*

Microsoft Exchange

TCP/IP Administration

Digital Systems

Technical Expertise

Operating Systems

*Windows (all versions),
Linux/Unix*

Languages

*.NET, c#, c/c++, Java,
Assembly, RS232/RS485*

Protocols & Services

*TCP/IP, HTTP(s), (s)FTP,
SMTP, POP3, DNS, IMAP,
SCP, SSH*

Cory Dixon, Principal Consultant

Mr. Cory Dixon is a Principal Consultant and has been working with information technology for over eight years and has shown himself to be a great wealth of information in the information technology and security tools arena. Mr. Dixon is a self-starting individual that takes great pride in understanding as much of information technology as one person can. Mr. Dixon's experience encompasses enterprise operations and security management, policies and standards, consulting, assessments, and penetration testing.

Mr. Dixon is the consultant you engage to learn, understand and improve your security tool sets. He has the motivation and energy to perform any task assigned. He has the ability to learn and understand multiple security tools, product and service and harness that knowledge to better serve an enterprise. His understanding of security far outweighs that of many of his peers in time and experience.

Key accomplishments

- Implementation of Vontu into enterprise network environment including day to day operations guides, product tuning and infrastructure design and roll-out
- Endpoint Security implementation expert with detailed knowledge of client computer requirements on upgrading to endpoint security products including, AV, FW, Vontu and Altiris.
- Day-to-day security tool operations, enhancements and maintenance of multiple security tool platforms.
- Performed various penetration tests on network and application based testing platforms
- Cisco Hacking- Performed an ethical hack on a high value Cisco Router where the client had stated the router failing would alert support. Resulting test changed the scope of how the boundary router security mechanisms were implemented
- Wireless Hacking- Provided Wireless Penetration supporting clients identifying rogue wireless access points and clients attempting connections to their corporate wireless network.
- Penetration testing on high value targets in secured environments.
- Web application testing for customer member bank member interface applications. Providing Ethical hacking on high net



EMAGINED SECURITY

Software

*Backtrack, Burp Suite,
Nessus, Netcat, Nikto,
OWASP ZAP, Snort,
Wireshark, Web Inspect,
Various other tools*

Certifications

*Certified Ethical Hacker
Certified*

A++ Certification

Vontu Certified

*Symantec Endpoint
Protection Certified*

PGP Certified

*Brightmail Gateway
Certified*

Altiris SE Certified

*Currently pursuing CISSP –
Certified Information
Systems*

*Certified Ethical Hacker
Certified*

Technical Specialties

Penetration Testing

802.11x Wireless

*Security Tool
Infrastructure Design,
Implementation and
Operation*

worth internet sites where customers have access to sensitive marketing and reporting of industry trend reporting.

- Symantec ESM 6.5, Bindview and Endpoint 12 Integration and Product Management Support. Provide support for product implementation and support including setup, training and identification of areas of use of product deployments.
- Responsible for customer training in various areas including; security, automation management, and programming control.
- Technical Support (SE) for consultant, sales department and upper management.
- Learned all past and present programming software and hardware specifications related to security and automation control systems.

Areas of Expertise

*Penetration Testing
(Application / Network)*

Software Development

Process Improvement

*Application Security
Mechanisms*

Network Design

Software Architecture

Secure Code Review

Log Review and Analysis

Technical Expertise

Operating Systems

Linux/Unix, Windows

Languages

*Java, Groovy, Ruby,
Python, c#, c/c++*

Protocols & Services

*TCP/IP, HTTP, FTP,
SMTP, SOAP & JSON web
services*

Hardware

Thales nShield HSM

Software

*Burp Suite, Nmap,
Nessus, Nexpose,
Wireshark, Netcat,
Sqlmap, Tomcat and
Apache web server,
Symantec PGP, Symantec
SEP*

Michael Losee, Senior Consultant

Michael Losee is a security consultant and software developer with expertise in executing penetration tests. Mr. Losee has conducted web application and network infrastructure penetration tests, developed comprehensive security plans, and implemented extensive IT security processes. His background in software development and system administration give him the deep understanding of a web developer, in addition to the offensive mindset of an ethical hacker. He excels at connecting client business goals with their risk management strategies and takes pride in his strict code of professional accountability.

Mr. Losee is an exceptionally gifted software developer that has a keen understanding for understanding how individual software programs work and can identify scope and create valuable software program structures. His key to developing these programs comes from his deep understanding of both the business logic and vulnerability analysis of hundreds of programs he has assessed.

Having such experience in both software development and penetration testing enables Mr. Losee to think outside the box in his review of any project put in front of him.

Key accomplishments

- Mr. Losee consistently identifies high risk vulnerabilities through his expertise with using automated tools, manual testing procedures, and developing custom scripts.
- Experience in Security Information and Event Management (SIEM); advanced event detection, correlation, triage, auditing, logging, and identifying malicious traffic to counter cyber threats, including attacks by the hacking group Anonymous.
- Designed and implemented an externally available security gateway which authenticated users, forwarded user meta-data, and routed users to internal applications via reverse proxy.
- Lead developer on a process improvement initiative to migrate a legacy COBOL mainframe application to a modern web application and integrate new processes, including secure code reviews and automated regression testing.
- Extensive log analysis review and log investigation experience.



EMAGINED SECURITY

Certifications

*Offensive Security PWB
Thales nCSE*

Symantec SEP

Symantec PGP

Technical Specialties

*Penetration Testing and
Customized Remediation
Guidance*

- Created two open source projects which extend the functionality of Nessus and Nmap.
- Successfully deployed, hardened, and administered Tomcat and Apache web servers on Department of Defense (DoD) infrastructure.
- Installation and configuration of Symantec PGP in corporate environments enabling customers to install an entire PGP infrastructure, create and deploy client packages in under the budgeted scope of time estimated for the project.
- Day-to-day security tool operations, enhancements and maintenance of multiple security tool platforms.
- Penetration testing on high value targets in secured environments.
- Extensive experience in documenting security architecture solutions, program SDLC lifecycle and software business requirements.
- Identified several zero day exploits in customer applications that had previously had full penetration tests and no critical vulnerabilities were identified.
- Responsible for customer training in various areas including; security, automation management, and programming control.
- Currently holds United States SECRET security clearance.



Areas of Expertise

*Ethical Hacking /
Penetration Testing*

*Vulnerability
Management*

*Vulnerability
Assessments*

*Network Architecture
Analysis / Design*

*Security / Risk
Assessment*

*Network, Application and
Perimeter Security*

Systems Administration

*Peer Training/Team
Mentorship*

Technical Expertise

Security Tools

Burp Suite

Hashcat

Metasploit

Nessus

Nikto

Nmap

PowerShell Empire

PowerSploit

SQLMap

Wireshark

Wfuzz

Arthur Borrego, Senior Consultant

Arthur Borrego is a senior security consultant with Emagined Security, providing expertise in the fields of Ethical Hacking/Penetration Testing. Prior to joining Emagined Security, Arthur Borrego served in a technical capacity at Nicklaus Children's Hospital as a Systems Administrator. Arthur Borrego comes from a diverse background and experience working with a wide array of technologies and enterprise products including but not limited to VMWare vSphere, Cisco UCS, Microsoft Exchange, Active Directory, Microsoft SCCM, Sophos SafeGuard, and Sophos Endpoint Security and Controls.

Key accomplishments:

- Lead tester on numerous penetration testing engagements.
- Mentored/trained team members on penetration testing/ethical hacking methodologies.
- Developed multiple Python scripts to automate repetitive tasks commonly encountered on penetration tests.
- Achieved "Guru" status and ranked in the top 100 in the "Hack The Box" penetration testing labs, which is a well-known educational platform for ethical hacking.
- Managed and grew a VMWare environment of about 50 hosts to over 300 hosts and 1500 + virtual machines.
- Developed and maintained security hardened baseline/golden images for multiple operating systems distributions of both Windows and Linux.
- Implement a light-touch Operating System deployment leveraging Microsoft SCCM.
- Implemented a phased monthly patching process for all workstations and servers with WSUS/SCCM integration.
- Maintained a Microsoft SCCM environment and managed over 5000 servers and workstations, including patch management, OSD, and application delivery.
- Managed a Cisco UCS infrastructure spanning four UCS domains and over 200 blade servers.
- Developed and implemented numerous Active Directory GPO policies and ACLs.
- Lead initiatives to automate various Active Directory tasks using PowerShell scripting.
- Successfully completed a project to implement and maintain hardware encryption using Sophos SafeGuard Encryption.
- Implemented and maintained Sophos Endpoint Security and Control.



EMAGINED SECURITY

***Technical Expertise
cont.***

***Programming
Languages***

PowerShell

Python

Product Experience

Active Directory

Cisco UCS

Microsoft Exchange

Microsoft SCCM

Sophos

VMWare vCenter

VMWare vSphere

Certifications

OSCP, KLCP

*CCNA, CCNA Security
(Expired)*

CompTIA A+, N+, Security+

Education

*Western Governors
University (B.S.)*

- Managed and successfully completed projects to migrate over 3000 workstations to Windows 7 and then again to Windows 10.



Areas of Expertise

*Ethical Hacking /
Penetration Testing*

*Vulnerability
Management*

*Vulnerability
Assessments*

*Security / Risk
Assessment*

*Network, Application and
Perimeter Security*

*Problem Solving –
Concrete & Abstract*

Analytics and Research

Documentation

*Law Enforcement
Relations and
Collaboration*

MITM attacks

*Local and Remote
Privilege Escalation*

Technical Writing

Certifications

CEH, A+

Education

*Western Governors
University - BS in
Information Security -
Degree Expected
December 2019*

Mitchell Stephens, Consultant

Mitchell Stephens is a security consultant with Emagined Security, providing expertise in the fields of Ethical Hacking/Penetration Testing.

Mr. Stephens brings five years of experience in the cyber security field and has led and managed 50+ penetration tests in all facets of the industry. In addition to leading penetration tests, Mitchell Stephens has also conducted many configuration reviews on critical perimeter and network management devices.

Along with expertise in Cyber Security, Mr. Stephens also has a strong English background. He has studied technical writing, along with interpersonal communications. He will be able to clearly and concisely convey the information that needs to be shared.

Key accomplishments

- Lead and managed 50+ penetration test and vulnerability assessments. Many involving compromise of the affected environment.
- Supported Emagined Security SOC operations on a variety of services including Symantec SEP, Fortinet Firewalls and Symantec Message Gateway.
- Conducted many configuration reviews of various network devices, providing critical information to strengthen the overall security of the tested environments.
- Strong expertise in the following tools:
 - Nmap
 - Nessus
 - Metasploit
 - Nipper
 - Kali Linux Toolbox



EMAGINED SECURITY

Areas of Expertise

*Ethical Hacking /
Penetration Testing*

*Vulnerability
Management*

*Vulnerability
Assessments*

Digital Forensics

*Security / Risk
Assessment*

*Network, Application and
Perimeter Security*

*Problem Solving –
Concrete & Abstract*

Documentation

Social Engineering

Web Development

Certifications

*SLAE, SPSE, SJSE, PCNSE,
CCNA (R&S), Pentest+,
CySA+, Sec+, Net+, A+*

Education

*Johnson County
Community College
(Grad. 2022)*

Centriq Training

Dom Allen, Principal Consultant

Dom Allen is a Principal Security Consultant with Emagined Security with more than 6 years of proven information security experience. After being an integral blue team member in a network operations center, Mr. Allen opted for a more offensive role, where he realized a deep passion that lent itself to naturally accelerated growth within the field. Mr. Allen's devotion to problem-solving and out-of-the-box creativity has helped him identify and report multiple security vulnerabilities to multiple bug bounty programs.

As an active member of Kansas City's longest-running monthly security meetup, Mr. Allen often delivers rigorous reports to executives employed by several Fortune 300 companies and leads talks to better inform local cyber security professionals in the group. Additionally, Mr. Allen actively analyzes consumer devices, such as Roku, Nikon cameras, garage door controllers, and smart entry systems akin to the Amazon Ring, for security weaknesses.

Key accomplishments:

- Contributed more than a dozen unique vulnerabilities to open source bug bounty programs and many more unpublished ones that had been discovered by others.
- Architect of modular, responsive, elegant systems for myriad use-cases, including custom Command and Control back-ends, surreal phishing guises with effective results, as well as intricate payload delivery systems that thwarted Top 10 security appliance vendors.
- Effective, driven tester with a proven track record on numerous penetration testing engagements, including social engineering, physical and perimeter assessments, lock bypass demonstrations, and custom exploitation development for bench-marking security controls at an unparalleled standard with multiple Fortune 300 clients.



EMAGINED SECURITY

Areas of Expertise

Penetration Testing

Cyber Threat Analysis

Vulnerability Management

Vulnerability Assessment

Red Team/ Adaptive Threats

Digital Forensics

Security / Risk Assessment

Process Development

Symantec Endpoint Protection/Two Factor Authentication

SIEM Analysis

Technical Writing

Incident Response

Symantec Backup Exec

Network, Application and Perimeter Security

Problem Solving – Concrete & Abstract

Analytics and Research

Program Creation, Management and Development

Social Engineering

Documentation

Clearance

Secret Clearance (DoD)

Ishmael J. Malik, Consultant

Ishmael J. Malik is a security consultant with Emagined Security, providing expertise in the fields of Ethical Hacking, Proactive Network Testing, Cyber Security Threat Management Analysis, Security Information and Event Management (SIEM), Vulnerability Management, Incident Response, and Computer and Network Forensics. Prior to joining Emagined Security, Mr. Malik served in both technical and supervisory capacities at Aerojet Rocketdyne. Mr. Malik possesses strong skills in identifying client needs and fostering collaboration with multiple cross-functional teams to formulate and implement successful security solutions to complex organizational challenges. Mr. Malik is an effective communicator who excels at both written and verbal communication skills. Mr. Malik has demonstrated ability to bridge the gap between technical and non-technical personnel and brings with him an arsenal of experience working on a myriad of established and cutting-edge security technologies and hardware and software platforms.

Key accomplishments:

- Lead cyber threat and incident management liaison between client and Defense Cyber Crime Center (DC3) / Defense Industrial Base (DIB) that required risk analyses metrics, incident response, containment, mitigation, threat actor analysis, forensic acquisition and analysis, remediation techniques and implementation and collaboration with appointed Department of Security Services (DSS) and Federal Bureau of Investigations (FBI) agents. Malik worked across all aspects of the organization to ensure inline security controls were in accordance to recommendation and compliance.
- FireEye-MAS/WebMPS/EX appliance administrator, event monitoring, and incident response lead. Malik has contributed directly to implementation, compliance, documentation, and administration to all FireEye appliances deployed throughout the organization. Malik constantly updated all FireEye appliances with real time threat intelligence from Defense Intelligence Agency (DIA), National Security Agency (NSA), Defense Cyber Crime Center (DC3), Department of Homeland Security, Central Intelligence Agency (CIA), US Computer Emergency Response Team (US CERT), Federal Bureau of Investigations (FBI), iDefense Threat Intelligence, and Department Security Services (DSS), ensuring all perimeters



EMAGINED SECURITY

Education

*Sacramento, California
State University, BS –
Business Administration*

Industry Certifications

*Certified Ethical Hacker
(CEH) – EC-Council*

CompTIA A+ Certification

*Microsoft Windows
SharePoint Services 3.0,
New Horizons, 2008*

*Microsoft Office Share
Point Server 2007, New
Horizons, 2008*

*Windows SharePoint
Services Installation, New
Horizons, 2008*

*Windows SharePoint
Services Administration,
New Horizons, 2008*

- of the organization were secure.
- Appointed Cisco Proxy Admin. Malik created and maintained web policies, Custom URL Categories, web reputation and filtering, acceptable use controls, identities, routing and access policies throughout the infrastructure meeting customer's expectations for UAT of new controls and policies, and implementation.
- Forensic acquisition, analysis and data preservation. Malik utilized Guidance Software's EnCase for laptops, desktops, tablets, cell phones, storage devices, multiple platform servers and live memory collection and images through physical, logical, and remote acquisitions. Malik directly aided investigations through discovery of evidence and identification of indicators of compromise (IoCs) that have been shared with law enforcement organizations including DSS, FBI, and Air Force OSI.
- Malik provided technical support, security process and procedures development and maturation, direction, supervision and leadership to members of the PC support group and IT call centers. Malik contributed numerous knowledge-base articles and remediation guides for deskside support and the IT call center.
- Provided guidance and direction regarding security control elements in policies that included TLS, email encryption, phishing campaigns, Cyber Security awareness campaign, customer data exchange, overseas computing, and incident reporting.
- Technical writer for a Corporate Security Visitor Security Management implementation. Malik was selected to test and configure visitor security management software, peripherals, printers. Malik constructed supporting documentation for deployment and training for corporate security.
- Directed over \$500K in infrastructure resources. Malik instructed and trained peers as well as department employees with developed documentation and training that fosters to all learning altitudes at a technical and non-technical standpoint.

Areas of Expertise

*Ethical Hacking /
Penetration Testing*

*Vulnerability
Management*

*Vulnerability
Assessments*

*Fraud Detection /
Prevention / Control*

*Security / Risk
Assessment*

*Network, Application and
Perimeter Security*

*Problem Solving –
Concrete & Abstract*

*Program Creation,
Management and
Development*

Documentation

*Converged Environments
/ Cloud*

Social Engineering

Certifications

*CISSP, CCSP, SSCP, CEH,
Security+, Network+,
ITILv3*

Education

*Salt Lake Community
College (AS)*

*Western Governors
University (BS –
Cybersecurity and
Information Assurance)*

*Penetration Testing with
Kali Linux – Offensive
Security (OSCP)*

Xander Wright, Consultant

Xander Wright is a security consultant with Emagined Security, providing expertise in the fields of Ethical Hacking/Penetration Testing, Vulnerability Management, and Security/Risk Analysis. Prior to joining Emagined Security, Xander served as the Security Engineer for Boral North America, and on the Security Operations team for Intermountain Healthcare. Given Mr. Wright's diverse background and experience in enterprise environments, he is uniquely positioned to blend security and business advocacy into cohesive enterprise solutions with a high level of efficacy.

Key accomplishments:

- Mr. Wright has authored several different policies and procedures currently in use by different companies, including vulnerability management, acceptable use, data classification and retention, and incident response. In writing these, Mr. Wright worked closely with the affected departments to ensure a rapid and streamlined adoption of these policies.
- Mr. Wright served as the Lead Engineer for a comprehensive vulnerability management program for a 12,000-asset organization, creating the vulnerability management program from scratch, including the procurement of necessary software and hardware, policy documentation, and updating the change control process to better support the goals of the vulnerability management program.
- Mr. Wright served on a security operations center (SOC) team for a 180,000-asset company during the initial discovery and responses against WannaCry, BadRabbit, and Petya ransomware attacks, coordinating systems support and incident response to mitigate the damage as much as possible. Due to the work of the SOC and Mr. Wright's contributions, the organization was not impacted by any of the above malware.
- Mr. Wright received one of the first Capstone Excellence Awards from his alma mater in the history of the Cybersecurity program for his project on building out an environment designed for highly dynamic collaboration between internal red and blue teams in a purpose-built, virtualized environment to allow for continual



improvements of both the red and blue team's efforts to improve the security posture of the company, including gathering the hardware necessary, configuring the software, and writing the policy and documentation accordingly.



EMAGINED SECURITY

Areas of Expertise

*Ethical Hacking /
Penetration Testing*

*Vulnerability
Management*

*Network, Application and
Perimeter Security*

*Systems Administration /
Integration*

*Network Architecture
Analysis / Design /
Migration*

Troubleshooting

Analytics and Research

Documentation

Certifications

*Certified Ethical Hacker
(CEH)*

*Microsoft Certified
Professional (MCP)*

CompTIA A+

Education

*Pioneer Pacific College
(AAS - Computer
networking technologies
and troubleshooting)*

Barton Allison, Consultant

Barton Allison is a security consultant with Emagined Security, providing expertise in the fields of Ethical Hacking/Penetration Testing, Systems Administration, and Security/Compliance. Prior to joining Emagined Security, Mr. Allison was a consultant for 15 plus years in small and medium businesses. He was also a lead engineer for Stairmaster/Startrac/Schwinn, an international manufacturer of exercise equipment, merging multiple business networks together. He was also a support specialist for audiologists and dentists across the country specializing in HIPPA compliance. Mr. Allison's executive level quality of support, communication and prompt, patient communication is highly sought by the clients who have worked with him.

Mr. Allison is an analyst with a demonstrated ability to troubleshoot complex security issues. He has an uncanny ability to dive into new technology without hesitation and employ a wholistic view that encompasses all aspects of the solution. Mr. Allison has the ability to bridge the communication gap between support companies, local technicians, and end users. Mr. Allison has been sought after and praised for his contributions to information security at each organization he has worked. He brings daily passion, confidence, and positivity to his work. Mr. Allison also puts his clients at ease by listening to them and educating them on their concerns and ensures that every Emagined Security client feels comfortable with him and his work.



EMAGINED SECURITY

Areas of Expertise

*Cloud Infrastructure
Security*

*VMware, vCloudAir,
Amazon, Digital Ocean,
Vultr*

*Application Development
in Perl, Python and
GoLang*

*M&A life cycles, driving
from due diligence,
integration planning, and
tactical execution*

*Solid understanding of
firewall configuration,
implementation and
intrusion detection.*

*Next Generation
technologies and non-
traditional use cases*

*Experience with a vast
array of common and
cutting edge storage
technologies and
platforms.*

Electronic Investigations

*Management of a 20
person, geographically
distributed Security
capability, including
physical, electronic and
product security.*

*Security architecture and
strategic planning*

Executive CISO

Nicholas Albright, VP MSS

Mr. Nicholas Albright is a proven leader with extensive experience in planning, developing and implementing unique technical and logical security initiatives that serve both early stage to late stage organizations. Mr. Albright has served as an executive Chief Intelligence and Security Officer focused on the development and execution of an achievable intelligence driven security program. Mr. Albright has over 15 years of hands on technical experience working in large scale corporate network environments and over 7 years of hands on technical experience working in virtual and cloud environments.

Key accomplishments

- Developed and Managed Intelligence Driven Information Security Practice for a large multi-national virtualization company.
- Developed Security Metrics for executive leadership and the board using Lockheed Martin's Kill Chain approach.
- In depth investigation, attribution and disruption of Nation State Adversaries (aka APT)
- Developed Adversary lexicon to track Tactics, Techniques and Procedures cohesively through the STIX model
- Authored and maintained Zero Premise security control technologies for early warning detection of suspicious recon events.
 - PassiveDNS/NOD
 - Domain Brand Awareness
 - Credential Theft
 - Malware Sinkholes
- Developed the first bidirectional automated intelligence sharing tools between private industry and US CERT.
- Reduce Overall Security Spending by ~5M through use of Open Source and home grown solutions.
- Developed Operational Intelligence capability to monitor Social Media, Darknet and Clearnet for compromises.
- Anomali University Threat Intelligence Instructor
- Regularly present on Threat Intelligence strategy and adversary disruption for organizations, ISACs and security venues
- Founded Shadowserver, a Non-Profit entity which monitors and reports on adversary activity. (No longer affiliated)
- Developed Threat Lexicon for cross collaboration between vendors and customers.



EMAGINED SECURITY

Skill Description

Extensive Research on State Sponsored Adversaries

Counter Threat Research for Adversary Tracking and Profiling

Ten years of experience as an Incident Response Investigator

Twelve years of Malware Reverse Engineering and Botnet Monitoring

Fifteen years of penetration testing experience.

Open Source Advocate and Contributor

Former Credentialed Law Enforcement – Electronic Crimes

Developed Training programs for USSS, FBI, DOI, LAPD

Presenter at Bsid es Las Vegas, SANS and local Defcon Chapters

Awards and Memberships

Member: DShield, US-CERT GFIRST, Yasml, Drone Armies, OWASP, OPS-TRUST, Infragard

Certified Protection Officer (Executive Protection)

- Threat Intelligence Integrations including Tanium, Carbon Black, TrendMicro and Maltego
- Wrote and maintained dozens of Malware Config Dumpers
- SOC 2 Compliance
- Security Program based on NIST Framework
- Developed and managed a twenty person team of Penetration Testers, Intelligence Analysts and Security Analysts working in a joint Counter Threat capacity
- Introduced the concept of Supply Chain monitoring to prevent incidents caused by third party organizations
- Reduced risk by introducing proactive security monitoring strategies, OSINT and Full Scope Penetration Testing
- Redteam (Penetration Testing)
- Created Vulnerability Management and Bug Bounty programs on near zero budget.
- Managed Security Integrations for major M&A's, including security testing, remediation and policy frameworks.
- Cloud Computing Security Strategies
- SF85 BI and Drug Enforcement Agency (DEA) Clearance
- Computer Security Incident Response Senior Investigator
- SF85 MBI+DEA Clearance
- Extensive malware research and botnet tracking.
- Training and consultation for the US Secret Service, FBI and LAPD.
- Reverse engineering and behavioral analysis of malware.
- Developed and maintained relationships with Internet Service Providers.

Interests

- *Binary, web application, network and physical penetration testing.*
- *Reverse and social engineering as it pertains to computer security.*
- *Research, tracking and disruption of advanced threats*
- *Privacy and Open Source*

ATTACHMENT 2: Sample Report

<This Page Intentionally Left Blank>

Office of the Washington State Auditor

Entity 99 – Office of Paranormal Activity

Consolidated Penetration Test Report

Prepared For:

Agent Mulder
Office of the Washington State Auditor
19 February 2021

Prepared By:

Emagined Security
2816 San Simeon Way
San Carlos, CA 94070
650-593-9829



Revision History

Date	Version	Description	Author
12 February 2021	0.1	Initial report stub and consolidation template	Consultant One
15 February 2021	0.2	Report Review	Consultant Two
16 February 2021	0.3	Review Updates	Consultant One
16 February 2021	0.4	Report Review	Consultant Three
17 February 2021	0.5	Review Updates	Consultant One
19 February 2021	1.0	SAO Deliverable Draft	Consultant One



Table of Contents

Revision History..... 2

Executive Summary 4

Engagement Objective..... 7

Identified Vulnerabilities and Severities 8

Application 1 9

Application 2 21

Internal Network 30

Appendix A: Severity Classification and Methodology 40



Executive Summary

At the request of the Office of the Washington State Auditor (SAO) in conjunction with the Office of Paranormal Activity (Entity), Emagined Security consultants performed a penetration test of the Entity's selected internal and external applications and networks. The purpose of this engagement was to identify vulnerabilities attackers can leverage to compromise the environments of the associated applications and networks tested during the engagement period.

Engagement Period

Start: 01 February 2021

End: 12 February 2021

Engagement Team

Fox Mulder
Dana Scully

Administrative & technical contact
Technical contact

fox.mulder@sao-opa.wa.gov
dana.scully@sao-opa.wa.gov

Emagined Security consultants performed penetration testing on two (2) internal web applications during the course of this engagement. The applications tested were:

- Application 1
- Application 2

Additionally, Emagined Security consultants performed penetration testing on the Entity internal production network, as well as the wireless networks within the scope of the engagement.

The consolidated results from these testing efforts are detailed in this section of the report, which are then followed directly by the individual application and network penetration reports in their entirety. For detailed technical specifications for the individual testing efforts, please kindly refer to the corresponding technical reports.

Testing was conducted from the following attacker's perspective:

- attacker onsite at Entity's location (insider threat)
- remote attacker (external threat)

The results from this test apply to the Entity applications and networks, where applicable within the written scope of the engagement. Emagined Security consultants evaluated only those assets in scope. Findings summarized below are representative of security issues found and may not list all instances of a specific issue.

SAO and the Entity should bear in mind that penetration testing is a point-in-time effort and may not be comprehensive nor reflective of the overall Entity security posture. Vulnerabilities disclosed may improve, deteriorate, or remain static over time, based on mitigation activity.

In review of the vulnerabilities identified, and from discussions with the Entity point of contact identified above, Emagined Security consultants noted the following with respect to the Entity's assets within the confines of the testing engagement's scope, focus area, and the consultants' overall knowledge of the Entity environment:



Areas of Strength - The Entity exhibits the following strengths within the internal/external environment:

- Application 1 stood up very well to application penetration testing. It is obvious, based on application behavior that previous testing has occurred and the organization has hardened application user input filtering and business logic behavior. These traits are indicative of a mature application security mindset and would deter many casual attackers.
- Application 2 is resistant against many common application vulnerabilities, such as utilizing out-of-date software, misconfiguration issues, and weak password policies. Additionally, the application has no accessible webpages to unauthenticated users. This reduces the overall risk by limiting application visibility of a potential attacker and potential attack vectors within the application.
- The Entity's internal network is excellently prepared against common attacks that would lead to immediate compromise. Specifically, the testing sensor needed to be placed onto a privileged portion of the network to reach the tested assets. This greatly decreases the likelihood of a successful attack by limiting the amount of access that regular users have to the network. Additionally, Entity personnel are actively engaged and well aware of their duties, as it was noted that vulnerability management takes place on a regular basis.

Areas for Improvement - The Entity may increase its security posture within the internal/external environment by addressing the following:

- Application 1 should improve its response to unexpected or malicious input. Doing so will prevent injection issues, such as SQL injection. Additionally, common misconfiguration issues, while not as high of severity, can lead to significant problems when combined with other issues. Such is the case with clickjacking and arbitrary file upload, both of which present significant risk for loss of integrity within the application.
- Application 2 will benefit from migrating unencrypted traffic to encrypted channels, such as HTTP over TLS. Additionally, utilizing HSTS will prevent potential attackers from downgrading from HTTPS to HTTP. This will help to prevent information, including credentials, from being captured while in transit via man-in-the-middle attacks. Additionally, input validation methods should be improved within the application to prevent injection attacks such as cross-site scripting.
- The internal network will be improved by mitigating and avoiding common misconfiguration issues. Specifically, default credentials present attackers with easy access to applications and services within the network and should be mitigated at the soonest opportunity. Additionally, sending unencrypted data, including credentials, over services such as HTTP and FTP present a confidentiality issue, as there is potential for data to be captured while in transit via man-in-the-middle attacks. These services should be migrated to encrypted channels to ensure confidentiality of the data being sent across the network.

Emagined Security offers the following caveat to the above speculative statement regarding areas of strength and improvement: Care should be taken not to place undue significance on this report, or upon any single penetration test as conducted at a given point-in-time against select Entity assets as environments, systems, tests, and security are dynamic in nature. Rather focus should be placed on the Entity's holistic security posture, its boundary and perimeter security controls, and the application thereof of said controls over time.



Finding Synthesis

Findings from the internal and external engagement are summarized in the below table.

Findings listed are categorized from a technical perspective only and do not attempt to factor nor adequately reflect all security safeguards and countermeasures present or planned for the environment in which these findings were detected. The respective target organization will want to assess risk represented by the below findings independently and in accordance with its existing risk assessment program, that includes factors planned and present security controls wholly in relation to organizational risk appetite, accepted residual risk levels, and systems, assets, and data valuation.

Unless otherwise specified in the Rules of Engagement, manual and automated testing did not specifically include any availability-based attack vectors such as denial of service (DoS).

How to interpret the table: Finding refers to the named technical vulnerability identified; severity pertains to the impact realized from a successful exploit of the named vulnerability; difficulty refers to the level of skill needed to perform a successful exploit against the named vulnerability; disposition pertains to the current state of remediation for the vulnerability.

Application 1

Finding 1:	SQL Injection			
Severity:	High	Difficulty:	Hard	Disposition: Open
Finding 2:	Arbitrary File Upload			
Severity:	Medium	Difficulty:	Moderate	Disposition: Open
Finding 3:	Clickjacking (UI Redress)			
Severity:	Low	Difficulty:	Moderate	Disposition: Open

Application 2

Finding 1:	Unencrypted Application Traffic			
Severity:	High	Difficulty:	Moderate	Disposition: Open
Finding 2:	Cross-Site Scripting			
Severity:	Medium	Difficulty:	Moderate	Disposition: Open
Finding 3:	HSTS Not Enabled			
Severity:	Low	Difficulty:	Hard	Disposition: Open

Internal Network

Finding 1:	Cleartext Services			
Severity:	High	Difficulty:	Easy	Disposition: Open
Finding 2:	Default/Blank Credentials			
Severity:	High	Difficulty:	Easy	Disposition: Open
Finding 3:	Vulnerable SSH			
Severity:	Medium	Difficulty:	Moderate	Disposition: Open



Engagement Objective

Emagined Security contracted with the Office of the Washington State Auditor (SAO) to provide a penetration test of the selected Entity's internal applications and networks. Findings listed in the Identified Vulnerabilities and Severities section contain detailed results from the test and elaborate on those vulnerabilities directly affecting the security posture of the Entity environment.

Vulnerabilities disclosed within this document represent 'point-in-time' findings at the time of testing and are indicative of security issues encountered during the test window. These vulnerabilities are weighted against industry standards, Entity security policy, and the experience of Emagined Security consultants. As time progresses, this document will become less representative of the Entity 's environment due to changes in that environment, new vulnerability and exploit discovery and publication, and advances in technology and tools development.

Emagined Security utilizes the following criteria to provide SAO and the Entity with a better understanding of the security vulnerabilities within its environment:

1. Severity rating - based on the potential damage and exposure to the application and/or network if an adversary were to launch a successful attack using a given finding
2. Difficulty rating - based on the aggregate value of current security safeguards, the position of an attacker with the organization, and the knowledge necessary to carry out the attack using a given finding



Identified Vulnerabilities and Severities

The following charts provide a summation view of the overall engagement. These should help the SAO and the Entity better understand security concerns and issues detected within the environment, along with their base classifications, and apply the appropriate resources to address and resolve these issues based on urgency.



Application 1

Testing Parameters

Testing environment: production

Attacker perspective: attacker onsite at Entity's location (insider threat)

Authentication method: authenticated

Roles:

Admin
User

Administrative User
Standard User

The following Entity URLs were tested during the engagement:

<https://www.seti-contact.com>
<https://seti-mgmt.com>

Testing Narrative and Caveats:

The SETI Contact application is tasked with communicating with other-worldly entities. Authentication relies on form authentication and user tokens (cookies) to maintain session state. The application inputs primarily advanced mathematical user algorithms and outputs complex explanations of why something happened.



Critical Findings

CRITICAL findings may be used to immediately breach the integrity of the environment and/or the Entity. This level of severity should be addressed immediately.

No Critical Findings Identified



High Severity Findings

HIGH findings pose an increased danger to the Entity environment, and might currently be under attack. These findings may allow for the expedited exploitation of the target environment and should be addressed urgently.

Finding 1: SQL Injection

Severity: High

Difficulty: Hard

Class: Authentication

Internet Facing: No

Authenticated: No

Vulnerable Assets:

<https://www.seti-contact.com/inject/sql/statement.here> `sqli_parameter [parameter]`

Vulnerability Description:

The vulnerable application is susceptible to SQL injection.

SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements, or not strongly typed and thereby unexpectedly executed. It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another.

Once attackers realize that a system is vulnerable to SQL Injection, they may be able to inject SQL query and SQL commands through a vulnerable input form field or URL parameter to gain unauthorized access, or achieve levels of access or data extraction that would not normally be possible for non-vulnerable instances.

An attacker may also be able to execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of the database and/or expose sensitive information. Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data and system access for the attacker. It may be possible to manipulate existing queries, to UNION (e.g., command used to select related information from two tables) arbitrary data, use sub-selects, or append additional queries.

In some cases, it may be possible to read in or write out to files, or to execute shell commands on the underlying operating system. Certain SQL Servers such as Microsoft SQL Server contain stored and extended procedures (database server functions). With access to these procedures, attackers may gain access to the local system and run commands with administrative privileges.

[– Below is a sample application entry for reference purposes –]

(SolarWinds Example:)

Multiple SQL injection vulnerabilities in the Manage Accounts page in the AccountManagement.asmx service in the Solarwinds Orion Platform 2015.1, as used in Network Performance Monitor (NPM) before 11.5, NetFlow Traffic Analyzer (NTA) before 4.1, Network Configuration Manager (NCM) before 7.3.2, IP Address Manager (IPAM) before 4.3, User Device Tracker (UDT) before 3.2, VoIP & Network Quality Manager (VNQM) before 4.2, Server & Application Manager (SAM) before 6.2, Web Performance Monitor (WPM) before 2.2, and possibly other Solarwinds products, allow remote authenticated users to execute arbitrary SQL commands via the (1) dir or (2) sort parameter to the (a) GetAccounts or (b) GetAccountGroups endpoint.

For this instance, the GetAccounts endpoint, the 'dir' parameters is susceptible to stacked injections. By capturing the requests made by an admin user to the endpoint, authenticating as Guest and replacing the admin cookie with the Guest cookie, you can still make a successful request, and thus a successful exploitation vector for any authenticated user.



Being a stacked injection, this becomes a privilege escalation at the very least, as an attacker is able to insert his or her own admin user. A pull request for a Metasploit module which should achieve this on any product using the Orion service as the core authentication management system, using the GetAccounts endpoint, has been made available (<https://github.com/rapid7/metasploit-framework/pull/4836>). By default, the module attempts to authenticate as the Guest user with a blank password, then exploit the SQL injection to insert a new admin with a blank password.

This vulnerability was reported to Solarwinds on Dec 8th, 2014, and was assigned the CVE identifier CVE-2014-9566.

In this particular instance, Emagined Security testers were able to leverage this vulnerability to obtain backend database access from which they could then pivot and obtain domain administrator level credentials within the target network/environment.

Figure 1 - Sample caption:
[Image redacted]

Mitigation:

Addressing SQL injection should be performed in multiple steps:

1. Utilize parameterized queries. This keeps the query statement independent from the parameters by using placeholders for user data.

Parameterized queries consume data from the user and after validating them, assign them to corresponding parameters, which are already part of the SQL statement. This prevents user data from being passed into the SQL statement building process.

In pseudo code:

```
// receive data
username = sql.validate(request.username) // see user input validation

// query database
hash = sql.query("SELECT pass_hash FROM user_table WHERE user = %s", username)

// validate hash
hash = hash.validate(hash)
```

NOTE: The placeholder in SQL statement takes the username from the request and validates the input, subsequently placing it in the query string.

2. Implement stored procedures. These procedures are predefined, and similar to parameterized queries, use placeholders for parameter data.

Stored procedures may be used on predictable data sets. This may work for instances where specific values are consumed from known parameters such as drop-down menus. A function call is then made to the database with validated data. In the case of stored procedures, the SQL statement is built on the database server and not in the application layer of the execution stack.

In pseudo code:

```
// receive data
username = sql.validate(request.username) // see user input validation
password = sql.validate(request.password) // see user input validation

// query database
```



```
sessionID = query_creds(username, password)

//validate returned data
sessionID = sessionID.validate(sessionID)
```

3. Validate user input by testing type, length, format, and range. This includes any data sent in the client request, including non-editable input parameters, cookies and server headers.

Users may format input differently. For instance a phone number may contain a string with the following non-digit characters:

+ = () * ,

This data may also include white space. In the case of a phone number, the data should be properly typed for encoding, then parsed for integers/digits only.

Fields with more complex character sets should be parsed accordingly, and potentially dangerous characters should be stripped out as necessary, or properly typed.

Follow standard secure coding practices and validate return data to ensure it fits within the parameters' constraints and anticipated results. Depending on the data being read from or written to the database, the output returned from the call should be predictable and parsed for errors and/or other unexpected output.

Follow a 'least-privilege' model by ensuring the database is running with non-administrator system user access. In addition, ensure the database is properly encrypting credentials.

Follow recommendations from the database vendor for implementation specific controls to avoid SQL injection. Each database manages encoding differently, so what works on MS SQL may not work on Oracle, DB2, etc.

When necessary, review the application's source code, specifically where form validation takes place and ensure only the intended HTTP method(s) is/are accepted. Explicitly define acceptable HTTP methods for pages within the application.

Mitigation for SolarWinds issue:

Updates are available. Please see the References' vendor advisory for more information. Customers can obtain the latest version from the SolarWinds' Customer Portal.

1. Check the Release Notes for Orion NPM 11.5.
http://www.solarwinds.com/documentation/Orion/docs/ReleaseNotes/releaseNotes_11_5.htm
2. Review the system requirements and ensure the system aligns to the specifications.
3. Back up the affected database(s) (Microsoft KB: 2005, 2008, 2006 RD, 2012).
4. Check the upgrade path:
 - a. If only Orion is installed and the system is running NPM version 10.7 or higher, upgrading directly to 11.5 can proceed.
 - b. If NPM is running a version lower than 10.7, a stepped upgrade must be followed. For example if only NPM is installed, the stepped upgrade path would be as follows: Orion NPM 7.8.5 > 8.5.1 > 9.1 > 9.5.1 > 10.1.3 > 10.3.1 > 10.7 > 11.5.X.
 - c. If NPM is running in addition to other modules, make sure the Product Upgrade Advisor tool is checked to obtain an exact upgrade path for both NPM and the other modules to ensure compatibility is maintained.
5. Download the required versions from the customer portal, if required.
 - a. To download the current version, and any previous versions required, log in to the customer portal. Once logged in, use the License management menu to select 'My Downloads'.



6. Select the product to download:
 - a. Under the Server Downloads section, the latest release should be selected by default. If an earlier version is needed for the upgrade path, select it from the drop-down menu.
7. Run the installations, in order, to upgrade the product.

References:

Acunetix – What is SQL Injection:

<http://www.acunetix.com/websitesecurity/sql-injection.htm#what>

OWASP – Preventing SQL Injection:

http://www.owasp.org/index.php/Reviewing_Code_for_SQL_Injection

OWASP – SQL Injection Prevention Cheat Sheet:

https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet

SQL Injection – Wiki:

http://en.wikipedia.org/wiki/SQL_injection

MSDN – SQL Injection:

<http://msdn.microsoft.com/en-us/library/ms161953.aspx>

SQL Injection Walkthrough:

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

SolarWinds

NVD Reference:

<https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9566>

Exploit-Database Reference:

www.exploit-db.com/exploits/36262

CVE Search:

<https://cve.circl.lu/cve/CVE-2014-9566>

Sec Lists:

<http://seclists.org/fulldisclosure/2015/Mar/18>

Solarwinds Support:

[https://support.solarwinds.com/Success_Center/Network_Performance_Monitor_\(NPM\)/SolarWinds_Core_vulnerability_found_by_Nessus_scan_ID%3A_83817](https://support.solarwinds.com/Success_Center/Network_Performance_Monitor_(NPM)/SolarWinds_Core_vulnerability_found_by_Nessus_scan_ID%3A_83817)



Medium Severity Findings

MEDIUM findings do not pose an imminent threat to the Entity environment; however, when combined with other issues, they may lead to significant problems.

Finding 2: Arbitrary File Upload

Severity: Medium

Difficulty: Moderate

Class: Logic Attack

Internet Facing: Yes

Authenticated: Yes

Vulnerable Assets:

`https://www.seti-contact.com/share/all/the/secrets.here` `secrets_here [parameter]`

Vulnerability Description:

The application permits the uploading of arbitrary files.

Arbitrary file uploads permit an authenticated site user, including an attacker to upload files to the system that the application had not otherwise intended to accept or for which it was not expecting (e.g. a modified file extension). Arbitrary file uploading can occur as a result of several scenarios but is generally the result of a misconfiguration or flaw in the business logic/design of the application on the part of the developer/development team.

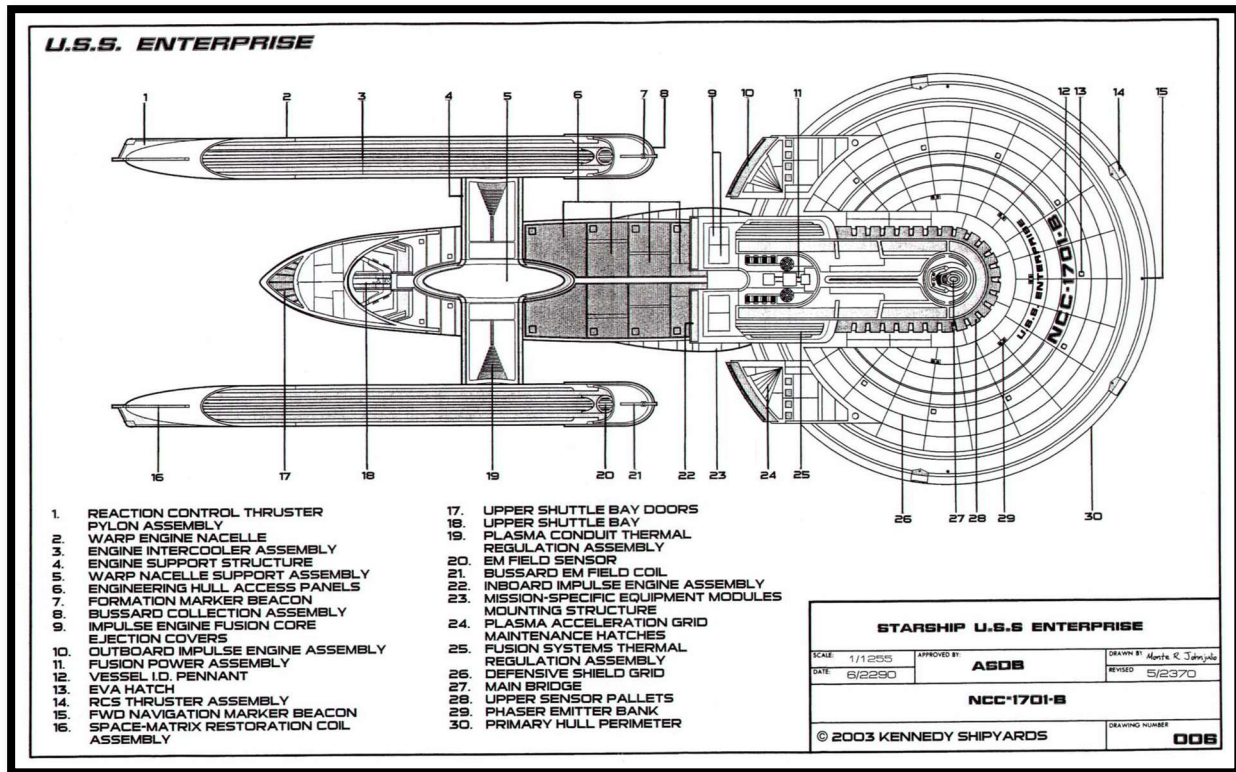
An attacker could use this vulnerability to stage and serve malicious files or content from the target system or application. Leveraging this issue, an attacker may also be able to infect or adversely impact other legitimate users of the application, sometimes without their knowing. The impact and severity of this attack often depends on the design of the application and the limits of the attacker's creativity and cruelty.

In this particular instance, the SETI Contact application allows for the uploading of non-algorithmic functions to include Starship schematics. Emagined Security testers uploaded design schematics for the now, outdated NCC-1701 (USS Enterprise), potentially providing old technology to a less advanced civilization.

The application does support client-side checks, which may be easily bypassed through a proxy or direct manipulation of the client-side JavaScript. The server does not appear to be validating the ELF headers of the file upload, nor does there appear to be any data-loss prevention (DLP) mechanisms in place to prevent the transfer of controlled intellectual property.



Figure 2 – Upload of NCC-1701 schematics file by simply appending filename with a permitted extension:





Mitigation:

The application currently utilizes client-side file-type checks, however this will not prevent a skilled attacker.

SAO/OPA should implement robust allow-listing for all permitted file types. All other file types not permitted should be explicitly denied.

Allow-listing checks should occur at the file header level (i.e., interrogate the file header construct) in addition to simply validating the proper file extension type is present to limit further trivial bypass. Allow-listing should also be applied in conjunction with other protective controls as by itself, it is not sufficient mitigation.

Files uploaded to the system should be placed in an isolated directory separate from other partitions on the filesystem and scanned with anti-virus and anti-malware software prior to any backend action being taken. Additionally, files uploaded to the system should then be renamed and copied to another portion of the filesystem where the end user does not have access and from which he or she cannot directly call or source the file, even in the event the renamed file name can be deduced or extracted.

Consider elimination of any file upload execution capability by limiting the ability to execute uploaded files from within the upload directory, if possible. For image files, consider re-compressing them using a secure library to ensure they are valid image formats/types.

Leverage the Content-Type header, but understand that it can be modified or changed client-side, so reliance on it singularly or as a primary means to contain arbitrary files should be avoided.

Finally, ensure appropriate file upload permissions are set on all uploaded files and directories.

Alternatively, SAO/OPA should review its file upload capabilities within the respective application and eliminate any upload capability that is not essential to the application's function/business purpose.

References:

OWASP – Unrestricted File Upload:

https://www.owasp.org/index.php/Unrestricted_File_Upload

Web Application Security Consortium – Abuse of Functionality:

<http://projects.webappsec.org/w/page/13246913/Abuse%20of%20Functionality>

CWE-434: Unrestricted Upload of File:

<https://cwe.mitre.org/data/definitions/434.html>



Low Severity Findings

LOW findings do not pose a threat to the Entity environment. They do provide knowledge regarding the environment or its assets, and may be used to further the means of exploiting MEDIUM and/or HIGH severity findings, or chained together to increase the overall severity.

Finding 3: Clickjacking (UI Redress)

Severity: Low

Difficulty: Moderate

Class: Client-Side Attack

Internet Facing: Yes

Authenticated: No

Vulnerable Assets:

<https://www.seti-contact.com/login.html>

Vulnerability Description:

The affected assets are vulnerable to a UI Redress/Clickjacking attack.

Clickjacking is a malicious technique of tricking web users into clicking on something different from what the users perceive they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web page links/web pages. It is a browser security issue that is a vulnerability across a variety of browsers and platforms. A clickjack takes the form of embedded code or scripts that can execute without the user's knowledge, such as clicking on a button that appears to perform another function.

The vulnerable site is framed in a transparent iframe that is put on top of what appears to be a normal page. When users interact with the normal page, they are unwittingly interacting with the malicious site as well.

Utilizing a technique called frame busting it is possible to eliminate the possibility of valid users providing attackers with session or credential information. However, this type of defense by itself is normally ineffective and can usually be circumvented by a skilled attacker. In 2009, Microsoft introduced a new HTTP header, X-Frame-Options. This header can take the values DENY, SAMEORIGIN, or ALLOW-FROM *origin*, which will prevent any framing, prevent framing by external sites, or allow framing only by the specified site, respectively.

To test whether a site is vulnerable to clickjacking, create an HTML page similar to the following. Change the URL highlighted in red to point to the desired target site:

```
<html>
<head>
<title>Clickjack test page</title>
</head>
<body>
<p>Clickjacking Proof of Concept</p>
<iframe src="http://localhost:8080" style="width:100%;height:90%"></iframe>
</body>
</html>
```

If the text "Clickjacking Proof of Concept" appears at the top of the page, the target site is vulnerable. With a clickjacking defense script installed, the affected site should break out of the site that is framing it and that text will not be displayed. If the user's browser has JavaScript turned off, the target site should display nothing at all.

Figure 3 - Sample caption:

[Image redacted]



Mitigation:

Configure the application or web server to set the X-FRAME-OPTIONS=Deny HTTP response header that indicates the desired (target) site is unwilling to be framed.

The following check should be used when loading pages:

```
<head>
<style> body { display : none;} </style>
</head>

<body>
  <script>
    if (self == top) {
      vartheBody = document.getElementsByTagName('body')[0];
      theBody.style.display = "block";
    } else {
      top.location = self.location;
    }
  </script>
</body>
```

Note: this should be used in combination with the X-FRAME-OPTIONS=Deny response header as well.

References:

OWASP Clickjacking:

<http://www.owasp.org/index.php/Clickjacking>

CWE-693: Protection Mechanism Failure:

<http://cwe.mitre.org/data/definitions/693.html>

CAPEC-103: Clickjacking:

<http://capec.mitre.org/data/definitions/103.html>

Frame Busting:

<http://seclab.stanford.edu/websec/framebusting/>



Informational Findings

INFORMATIONAL findings are not direct threats to Entity information security; however, they deviate from what would be expected in a typically sized and secured environment.

No Informational Findings Identified



Application 2

Testing Parameters

Testing environment: non-production

Attacker perspective: attacker onsite at Entity facilities (internal threat)

Authentication method: unauthenticated

Roles:

Admin
User

Administrative User
Standard User

The following Entity URLs were tested during the engagement:

<https://www.seti-contact2.com>
<https://seti-mgmt2.com>



Critical Findings

CRITICAL findings may be used to immediately breach the integrity of the environment and/or Entity. This level of severity should be addressed immediately.

No Critical Findings Identified



High Findings

HIGH findings pose an increased danger to the Entity environment, and might currently be under attack. These findings may allow for the expedited exploitation of the target environment and should be addressed urgently.

Finding 1: Unencrypted Application Traffic

Severity: High

Difficulty: Moderate

Class: Authentication

Internet Facing: No

Authenticated: Yes

Vulnerable Assets:

<https://www.seti-contact2.com>

Vulnerability Description:

The vulnerable application is using insecure, cleartext services and protocols.

Cleartext protocols and services, such as HTTP, FTP, Telnet, and TFTP are inherently flawed in that they send all data across the wire in the clear, including any authentication information such as credentials. Any confidential data transferred such as personally identifiable information (PII), or other non-public information (NPI) and account data in the same session may also be captured or disclosed.

Attackers who are able to intercept or eavesdrop on in-the-clear transmissions are likely to compromise user information including login credentials and any other sensitive or potentially sensitive data transmissions. The level of effort to capture this detail by a skilled attacker is fairly trivial and can be accomplished using freely available tools and utilities.

In this instance, Emagined Security consultants confirmed the presence of unencrypted application communications within Application 2.

Figure 4 - Sample caption:

[Image redacted]

Mitigation:

In general, the recommended method of mitigation is to utilize a secure alternative to the insecure transport mechanisms currently in use. Secure alternatives typically all rely on the transport layer security (TLS) protocol.

HTTPS (HTTP over TLS) may be used to protect all HTTP communications, for instance, including forms-based and Basic Authentication implementations. This is often achieved through a simple web server configuration change.

When implementing TLS, be sure to avoid common pitfalls associated with SSL configurations:

- Ensure valid certificates are used for host identification and do not use wildcard certificates.
- Utilize the TLS v1.2 protocol specification or higher where possible. This includes explicitly disabling the SSLv2 and SSLv3 protocols. Both older versions and TLS versions prior to 1.2 have been found to be vulnerable or more susceptible to attack.
- Only utilize strong TLS ciphers. Those ciphers considered strong are 128 bits or greater, not to include the Rivest Cipher 4 (e.g. RC4-MD5 or RC4-SHA) cipher suites that are known to be vulnerable to certain types of SSL/TLS attacks.
- Ensure TLS compression is disabled where web applications may be passing session identifiers in cookies. This will help to prevent specific SSL attack vectors such as the BEAST and CRIME attacks, which seek to derive session identifiers in this manner.



References:

OWASP Transport Layer Protection Cheat:

https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.md

OWASP HTTP Strict Transport Security:

https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.md

WASC-04 – Insufficient Transport Layer Protection:

<http://projects.webappsec.org/w/page/13246945/Insufficient%20Transport%20Layer%20Protection>

CWE-319: Clear-text Transmission of Sensitive Information:

<http://cwe.mitre.org/data/definitions/319.html>

Microsoft – How to Set Up SSL on IIS 7:

<http://www.iis.net/learn/manage/configuring-security/how-to-set-up-ssl-on-iis>

SSL Support Desk – Windows Server 2012 – IIS 8 & 8.5 SSL Installation:

<https://www.sslsupportdesk.com/ssl-installation-instructions-for-windows-iis-8-and-8-5/>



Medium Findings

MEDIUM findings do not pose an imminent threat to the Entity environment; however, when combined with other issues, they may lead to significant problems.

Finding 2: Cross-Site Scripting

Severity: Medium
Internet Facing: No

Difficulty: Moderate
Authenticated: Yes

Class: Client-Side Attack

Vulnerable Assets:

<https://www.seti-contact2.com>

Vulnerability Description:

The affected application is vulnerable to cross-site scripting (XSS).

Cross-site scripting (XSS) occurs when unchecked user input is reflected back to the user and interpreted by the browser. Attackers may leverage this type of attack for phishing, cookie stealing, malware dispersal, or for other deviant purposes resulting in potential or realized damage to client systems and to the company brand.

Reflected or non-persistent XSS simply means the exploit does not remain on the server, thus reducing the attack surface and the overall magnitude of the attack's scope. However, there are tools available to attackers that can leverage an XSS channel even with a non-persistent XSS attack. This is an interactive communication channel between two systems, which is opened by an XSS attack. If successful, the attacker is then able to control the victim's browser. After this point the attacker can see requests, responses and is able to instruct the victim's browser to carry out requests.

Stored or persistent XSS is saved on the server after the attack and is considered the more severe form. Persistent XSS' effects can be far-reaching as the attacker's malicious script is rendered automatically without the need to individually target victims or lure them unknowingly to a third-party website; instead the script is delivered on the impacted system directly. Were the impacted system an otherwise trusted website with large traffic volume/visitation and a high number of unique users, the power of a successful persistent XSS attack could be realized quickly.

DOM-based XSS is a third variant that does not rely on malicious data touching or accessing the web server, and is not as ubiquitous as the other variants. In a DOM-based XSS attack, the malicious data is being reflected by the JavaScript code on the client-side.

Emagined Security consultants confirmed that there was persistent cross-site scripting when creating a 'ghost' within the applicable application parameter.

Figure 5 - Sample caption:
[Image redacted]

Mitigation:

There are several methods to employ to reduce the attack surface for this type of vulnerability: filtering, encoding/escaping and input validation.

Filtering may take place before the request reaches the application. Consider allow-listing parameter values. For instance, a name field should generally not include parameters which contain special characters, the obvious exceptions being hyphens or apostrophes sometimes used in surnames/family names. Filtering may also be achieved through introduction of an application firewall or a similar security appliance that has been tuned to



detect and filter unexpected or malicious input; this type of control measure often comes with additional costs and overhead to operate and maintain so it should not be opted for without additional cost analysis and business impact.

Encoding/Escaping is the method of URL encoding all special HTML characters so the client browser does not render the code passed back to the browser.

Input validation checks the user-supplied data with the application to ensure it fits within the parameters of the input field. For example, a phone number should only contain a specific number of positive integers.

Finally, all affected input fields should be evaluated to make sure they are necessary for the application to function. Methods for storing data such as in a cookie or retrieved from a user profile on the backend of the application should be explored to further bolster data protection.

References:

OWASP Top 10 2017 – A7-Cross-Site Scripting:

[https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A7-Cross-Site_Scripting_\(XSS\)](https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A7-Cross-Site_Scripting_(XSS))

Web Application Security Consortium – Cross-Site Scripting:

http://www.webappsec.org/projects/threat/classes/cross-site_scripting.shtml

CWE-79 – Improper Neutralization of Input During Web Page Generation (XSS):

<http://cwe.mitre.org/data/definitions/79.html>

OWASP – Cross-Site Scripting:

<https://owasp.org/www-community/attacks/xss/>

jQuery DOM-Based XSS Example:

<http://bugs.jquery.com/ticket/9521>



Low Findings

LOW findings do not pose a threat to the Entity environment. They do provide knowledge regarding the environment or its assets, and may be used to further the means of exploiting other MEDIUM and/or HIGH severity findings, or chained together to increase the overall severity.

Finding 3: HSTS Not Enabled

Severity: Low

Difficulty: Hard

Class: Configuration

Internet Facing: No

Authenticated: Yes

Vulnerable Assets:

<https://www.seti-contact2.com>

Vulnerability Description:

The vulnerable site/application does not employ HSTS.

HTTP Strict Transport Security (HSTS) is an optional security transport enhancement enforced at the HTTP response header level that, among other things, helps to ensure that any requests made over HTTP to the HSTS-enabled site/domain are instead routed over the more secure HTTPS protocol.

When an HSTS-aware web browser receives a request to utilize HSTS, it will prevent any further communications from being sent over HTTP to the specified domain and will ensure only HTTPS sessions are used instead. Other benefits of HSTS include the prevention of HTTPS click-through prompts, recognition and access to web sites running with valid only (i.e. no expired) SSL certificates, and protection from the ability to override invalid certificate messaging.

Without a site's using HSTS explicitly, it may be possible for an attacker to negotiate the site down from using HTTPS to HTTP for some communications by using attack vectors such as that afforded by sslstrip and similar tools. Additionally, other attacks that rely on HTTP attack vectors are still possible, including injection-based attacks.

The use of the HSTS directive is not without its own security considerations, however. Specifically, site owners can use HSTS to identify users without cookies; this can have privacy concerns. As cookies can also be manipulated at the sub-domain level, omitting the `includeSubDomains` directive from the HSTS response header can also lead to a broader range of cookie-based attacks. In this regard, it is essential for any sites leveraging cookies to ensure they employ the `Secure` flag on all cookies to further limit the success potential for these cookie-based attacks. The use of wildcard SSL certificates can also present some interesting challenges when considered in conjunction with HSTS. See the References section of this finding for additional information.

Mitigation:

To enforce HSTS on the site/current domain and all its subdomains, leverage the below syntax by adding it to the server's configuration, or alternatively, to the desired application's code. As some web servers' syntax will vary, consult the appropriate vendor documentation or website as needed:

```
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

NOTE: Some web browsers may ignore the `Strict-Transport-Security` header when accessing a site over HTTP. This is generally due to the fact that an attacker may be able to intercept HTTP connections and inject the header or remove it as desired. As a result, the Entity will want to consult the appropriate browser documentation when developing with specific web browsers in mind to ensure their behavior is in alignment with what the Entity anticipates.



Companies and organizations with a legitimate business need to run their sites with blended HTTP and HTTPS content should take precaution to thoroughly test all features and service calls with HSTS-enabled to ensure it does not cause unwanted behavior or worse, break the site.

Similarly, if there is any intention to return to using HTTP at any point in the future, use of the HSTS `preload` directive should be carefully considered in advance as it can have permanent results. See <https://hstspreload.appspot.com/> and specifically the 'Removal' section for more detail.

References:

OWASP HSTS Cheat Sheet:

https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html

RFC 6797 - HSTS:

<https://tools.ietf.org/html/rfc6797>

HTTP Strict Transport Security:

<https://https.cio.gov/hsts/>

NGINX – Adding HSTS:

<https://www.nginx.com/blog/http-strict-transport-security-hsts-and-nginx/>

Configure HSTS on IIS 7/8:

<https://www.tbs-certificates.co.uk/FAQ/en/hsts-iis.html>

Microsoft - IIS 10 HTTP Strict Transport Security (HSTS) Support:

<https://docs.microsoft.com/en-us/iis/get-started/whats-new-in-iis-10-version-1709/iis-10-version-1709-hsts>

HSTS for Apache, NGINX and Lighttpd:

https://raymii.org/s/tutorials/HTTP_Strict_Transport_Security_for_Apache_NGINX_and_Lighttpd.html



Informational Findings

The following findings are not direct threats to Entity information security; however, they deviate from what would be expected in a typically sized and secured environment.

No Informational Findings Identified



Internal Network

Testing Parameters

Testing environment: production

Attacker perspective: attacker onsite at Entity facilities (internal threat)

Authentication method: unauthenticated

The following Entity assets were tested during the engagement:

10.0.0.0/24



Critical Findings

CRITICAL findings may be used to immediately breach the integrity of the environment and/or Entity. This level of severity should be addressed immediately.

No Critical Findings Identified



High Findings

HIGH findings pose an increased danger to the Entity environment, and might currently be under attack. These findings may allow for the expedited exploitation of the target environment and should be addressed urgently.

Finding 1: Cleartext Services

Severity: High

Internet Facing: No

Difficulty: Easy

Authenticated: No

Class: Authentication

Vulnerable Assets:

FTP

10.0.0.19:21

computer19

10.0.0.99:21

<does not resolve>

Basic Auth over HTTP

10.0.0.1:443

computer1

10.0.0.244:8080

computer244

Cleartext Form

Authentication over HTTP

10.0.0.8:80, :443

computer8

Vulnerability Description:

The vulnerable assets are using insecure, cleartext services, authentication mechanisms, and protocols.

Cleartext protocols and services, such as Basic authentication over HTTP, FTP, Telnet, and TFTP are inherently flawed in that they send all data across the network in the clear, including any authentication information such as credentials. Any confidential data transferred such as personally identifiable information (PII), or other non-public information (NPI) and account data in the same session may also be captured or disclosed.

Attackers who are able to intercept or eavesdrop on in-the-clear transmissions are likely to compromise user information including login credentials and any other sensitive or potentially sensitive data transmissions. The level of effort to capture this detail by a skilled attacker is fairly trivial and can be accomplished using freely available tools and utilities.

In this instance, Emagined Security consultants confirmed the presence of FTP, Basic authentication over HTTP, and cleartext form login over HTTP.

NOTE: The above is not exhaustive. The Entity should confirm basic authentication over HTTP within every internal network segment and remediate accordingly

Mitigation:

In general, the recommended method of mitigation is to utilize a secure alternative to the insecure transport mechanisms currently in use. Secure alternatives typically all rely on the transport layer security (TLS) protocol.

HTTPS (HTTP over TLS) may be used to protect all HTTP communications, for instance, including forms-based and Basic authentication implementations. This is often achieved through a simple web server configuration change.

When implementing TLS, be sure to avoid common pitfalls associated with SSL configurations:



- Ensure valid certificates are used for host identification and do not use wildcard certificates.
- Utilize the TLS v1.2 protocol specification or higher where possible. This includes explicitly disabling the SSLv2 and SSLv3 protocols. Both older versions and TLS versions prior to 1.2 have been found to be vulnerable or more susceptible to attack.
- Only utilize strong TLS ciphers. Those ciphers considered strong are 128 bits or greater, not to include the Rivest Cipher 4 (e.g. RC4-MD5 or RC4-SHA) cipher suites that are known to be vulnerable to certain types of SSL/TLS attacks.
- Ensure TLS compression is disabled where web applications may be passing session identifiers in cookies. This will help to prevent specific SSL attack vectors such as the BEAST and CRIME attacks, which seek to derive session identifiers in this manner.

A note regarding Basic Authentication: While utilizing basic authentication over HTTPS does protect the header, the encoded string is sent with every request. This greatly increases the attack surface and the likelihood for offline or further reversing/decryption brute-forcing attacks. Depending on where TLS termination occurs within the affected environment, this string may be stored in proxies, load balancers, logs, and other networked devices at various points along the network communication path.

References:

OWASP Transport Layer Protection Cheat Sheet:

https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html

OWASP HTTP Strict Transport Security Cheat Sheet:

https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html

WASC-04 – Insufficient Transport Layer Protection:

<http://projects.webappsec.org/w/page/13246945/Insufficient%20Transport%20Layer%20Protection>

CWE-319: Cleartext Transmission of Sensitive Information:

<http://cwe.mitre.org/data/definitions/319.html>

Tecadmin – How to Set Up TLS on IIS 7:

<https://tecadmin.net/enable-tls-on-windows-server-and-iis/>



Finding 2: Default/Blank Credentials

Severity: High
Internet Facing: No

Difficulty: Easy
Authenticated: Yes

Class: Authentication

Vulnerable Assets:

Web Service 1

10.0.0.8:80, :443
10.0.0.12:80

computer8
computer12

admin:admin

Web Service 2

10.0.0.1:443
10.0.0.244:8080

computer1
computer244

root:root

FTP

10.0.0.19:21
10.0.0.99:21

computer19
<does not resolve>

[blank]:[blank]

Vulnerability Description:

The vulnerable assets leverage default credentials for authentication.

The systems and applications noted above are using default credentials that were supplied by the hardware and/or software manufacturer, or implemented/enabled off-the-shelf. As these default credentials are commonly published (i.e. there are websites purely dedicated to default credentials), easily obtained through trivial online searching, and routinely known to attackers and incorporated into most hacking tools, this places the vulnerable assets at unnecessary risk of compromise.

In addition to heightened risk of compromise due to the ubiquitous nature of the default credentials, their use has other information security ramifications including the loss of accountability and repudiation as it pertains to the system, hardware or software authentication employing the default credential. Their use also increases the complexity of incident response activities surrounding those assets utilizing default credentials, and contributes to a poor password policy.

In the case of FTP on those systems noted above, a user is able to enter any username and password, including blank or null passwords to gain access to the system.

In this instance, Emagined Security consultants confirmed the use of default credentials on multiple hosts using Web Service 1 and Web Service 2. Upon accessing Web Service 2, Emagined Security consultants had the ability to access device security configurations.

Mitigation:

Identify all systems, hardware, and software using default credentials within the impacted environment. Change the default credentials for every instance and ensure that change adheres to the Entity's password policy, and provides for a level of randomness so that a single password is not used for a particular product or platform across the enterprise.

Varying these credentials will further help to limit exposure and impact in the event a single credential is leaked, compromised or otherwise obtained illegitimately.

Reject all products that ship with default credentials that cannot be modified or changed, and work with the supplying provider, vendor or manufacturer to guarantee these credentials can be modified going forward. For all assets acquired with default credentials, policy and governance should be in place to guarantee these default



credentials are changed prior to the asset being placed onto the network or into rotation in a production or production-ready capacity.

References:

OWASP – Authentication Cheat Sheet:

https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

WASC-15 – Application Misconfiguration:

<http://projects.webappsec.org/w/page/13246914/Application%20Misconfiguration>

CWE-521: Weak Password Requirements:

<http://cwe.mitre.org/data/definitions/521.html>

CAPEC-70: Try Common (Default) Usernames and Passwords:

<http://capec.mitre.org/data/definitions/70.html>



Medium Findings

MEDIUM findings do not pose an imminent threat to the Entity environment; however, when combined with other issues, they may lead to significant problems.

Finding 3: Vulnerable SSH

Severity: Medium
Internet Facing: No

Difficulty: Moderate
Authenticated: No

Class: Vulnerable Application

Vulnerable Assets:

10.0.0.10:22	computer10
10.0.0.87:22	copmuter87

Vulnerability Description:

The affected assets are running with a vulnerable version of SSH.

Secure Shell (SSH) is a secure protocol for connecting two networked systems or hosts. SSH provides for the secure exchange or transmission of data, secure remote login/secure remote access, and secure remote command execution. SSH is broadly used to provide remote access and login capabilities chiefly amongst all other functionalities it provides. SSH was widely adopted as a secure alternative to insecure remote connection protocols such as telnet. SSH is not however without its own vulnerabilities and security challenges.

The version of SSH in use on the affected systems – OpenSSH 5.5 – is known to be vulnerable to eleven (11) (source from CVE) unique security issues, including denial of service and information disclosure. The general severity of these issues range from low to high and provide for partial compromise of confidentiality, integrity, and availability. For a complete listing of security vulnerabilities affecting the version of SSH in use, please refer to the CVE Details link in the References section of this finding.

Mitigation:

The version of SSH in use was released in April 2010. The current version of SSH is version 8.4, released in September 2020.

To instill as robust a security posture as possible for SSH and the internal environment, and to mitigate the security issues in v5.5, Emagined Security recommends downloading, testing, and deploying the current version of SSH.

Alternatively, if SSH came bundled with an operating environment and a support agreement has been secured or retained with the operating environment vendor, consider contacting the vendor for a custom support model that mitigates the issues facing the vulnerable version of SSH.

Ensure any implementations of SSH deployed within the environment or at the enterprise level are running secure protocol versions (2 or higher at the time of this report). SSHv2 should also not be configured to fail back to SSHv1.

References:

OWASP Top 10 2017 – A9-Using Components with Known Vulnerabilities:
https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A9-Using_Components_with_Known_Vulnerabilities



WASC-14 – Server Misconfiguration:

<http://projects.webappsec.org/w/page/13246959/Server%20Misconfiguration>

CVE – OpenSSH 5.5:

https://www.cvedetails.com/vulnerability-list/vendor_id-97/product_id-585/version_id-121221/Openbsd-Openssh-5.5.html



Low Findings

LOW findings do not pose a threat to the Entity environment. They do provide knowledge regarding the environment or its assets, and may be used to further the means of exploiting MEDIUM and/or HIGH severity findings, or chained together to increase the overall severity.

No Low Findings Identified



Informational Findings

INFROMATIONAL findings are not direct threats to Entity information security; however, they deviate from what would be expected in a typically sized and secured environment.

No Informational Findings Identified



Appendix A: Severity Classification and Methodology

Severity Classification

Each vulnerability identified in this report is labeled with a Severity ranking. These rankings are defined 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. An example of this type of system or data would be social security numbers, administrative passwords, or control of a primary server. Findings in this severity classification should be remediated immediately.
Medium	Findings at this level of severity could have a moderate impact to 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 Entity's proprietary/trade secret. Examples of these types of findings are internal anonymous FTP servers or organizational contact lists. 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. Examples of these types of findings are improper error handling messaging and default web pages/content that provide an attacker with direct knowledge of the server type, version and languages used so that he/she/they may reduce the amount of work needed in the attack. 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. Examples of these types of findings include HTTP header information disclosure, which can reveal web server and application frameworks in use. Findings in this severity should be considered for remediation at the earliest convenience.

Additionally, each finding identified is categorized as to the difficulty of exploitation. The difficulty of exploitation is subdivided into the following categories, in descending order of urgency:

Easy	Findings which 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 which require technical competency in the subject/field, and a moderate level of effort to reproduce the finding; goes beyond running an automated script or running public exploit code.
Hard	Findings which require the use of custom scripts, developed tools and/or procedures, advanced programming skills, and a detailed technical expertise or intimate subject matter familiarity.

It is important to note that the severity categorization and the difficulty of exploitation are independent. That is, while a given finding may result in significant business impact (High Severity) regardless, the difficulty level of exploitation to achieve that significant business impact may be either quite simplistic or quite skilled. While unskilled (i.e. low difficulty)



attacks at the higher severity levels should draw immediate concentration of resources to close them, it is understood that the more skilled the attacker is, the more persistent and specialized the threat to the organization becomes.

Testing Tools

Emagined Security uses a variety of automated and manual tools to increase the thoroughness and efficiency of the test. The following tools may have been used as part of this engagement:

- Portswigger Burp Suite Professional
- Tenable Nessus
- Offensive Security Kali Linux
- Rapid 7 Metasploit Network
- Various web browsers and plugins
- Custom scripts and proprietary tools

Methodologies

Emagined Security develops and employs multiple testing methodologies to provide and account for precision testing. Each methodology employed is specifically prepared for the type of testing engagement and its target environment(s), or tailored as a result from Emagined Security's previous experience and/or business requirements having formerly completed an engagement, or worked previously within the environment.

All methodologies used follow industry standards and share a commonly familiarity and foundation based on years of Emagined Security expertise in the industry. For a detailed description of the testing methodologies utilized for this engagement, please contact Emagined Security.

ATTACHMENT 3: Detailed Penetration Testing Methodology

<This Page Intentionally Left Blank>

Ethical Hacking / Penetration Test Methodology

Emagined Security
2816 San Simeon Way
San Carlos, CA 94070
650-593-9829

Ethical Hacking / Penetration Test Methodology

This document contains a general outline of the procedures to complete a vulnerability assessment / penetration test / ethical hack. Emagined Security defines each of the types of these tasks as follows:

- *Expanded Penetration Test (Level 3 – Red Team)*: This version includes the Defined Penetration Test and adds attempts to use the exploited vulnerabilities to compromise systems behind the initial targets. Additionally, Expanded Penetration Testing can be used to:
 - Evaluate the organization's security awareness
 - Validate the effectiveness of existing security controls
 - Attempt to compromise and / or circumvent security control undetected
 - Evaluate intrusion detection effectiveness
 - Assess incident response identification and response effectiveness
 - Test incident response capabilities

This is an exercise designed to demonstrate what an extremely skilled and dedicated attacker might reasonably accomplish during the testing period. This is the most extensive version of the test.

- *Defined Penetration Test (Level 2)*: This version includes the Vulnerability Assessment and adds exploitations of the vulnerabilities within the defined scope. This is the standard version of the test.
- *Vulnerability Assessment (Level 1)*: This version includes only scans and validation of vulnerabilities. It is minimal version of the test.
- *Vulnerability Scan (Level 0)*: This version includes a basic scan to satisfy regulatory requirements utilizing a single vulnerability tool. The associated deliverable is limited to only raw reports from the tool. No CONSULTANT analysis on results will be performed.

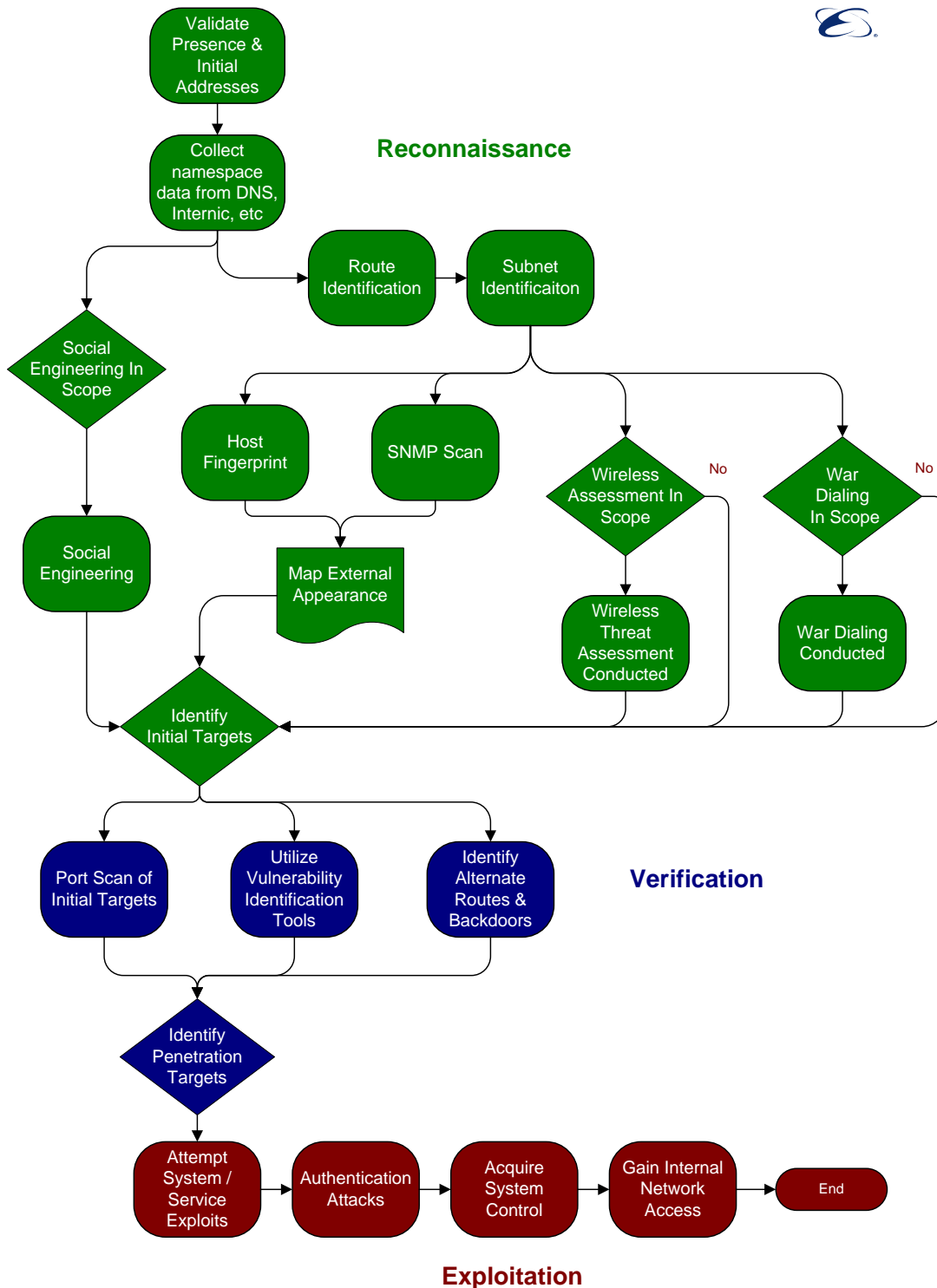
In this document, the versions of the test will be referred to as Penetration Tests. This document covers Emagined Security's Penetration Testing methodology at a high level; it does not enumerate the specific steps included in our procedures. Penetration tests are broken into three phases. While each phase is separate, not all phases are independent of each other. Some activities such as avoiding detection are listed as a separate phase, but they in reality typically also occur during all other phases of a test.

Before the penetration test begins the client must determine several parameters. These include:

- *Attacker Persona*: Will the penetration test mimic the actions of an outsider to the company, or a company employee, or some combination? For those studies coming from the outside efforts will center on only Internet connectivity, or will efforts such as partner locations be used as points to the network?
- *Methods Allowed*: The exact types of methods should be enumerated. This includes whether certain classes of attacks (e.g., Buffer Overflows, Denial of Service (DoS)) will be used.
- *Access to Results*: Who has access to the results of the test must be agreed upon beforehand. This also will limit those individuals that can be present during the actual test. (See monitoring below)
- *Systems Allowed*: This will identify the systems being tested and enumerate those specific systems that are "off limits" and cannot be tested.
- *Monitoring*: High level logs of activities must be kept and made available to the client. This also includes if the client must be present during all activities.
- *Professional Manner*: Company should require persons conducting test to act in a professional manner, meaning that they will not try attacks known to violate parameters established in the methods section and adhering to the C|EH or CISSP rules. Unprofessional conduct includes, for example, using known DoS attacks when DoS attacks have specifically been excluded.
- *Social Engineering*: Emagined Security does not routinely conduct "social engineering" attacks on customer support organizations because those are typically highly destructive. Emagined Security will work with a customer to design an assessment program that measures vulnerability to a social engineering attack without performing the deceitful activities commonly referred to as social engineering.

Phases of the Network Penetration Test

Penetration tests typically follow a structured approach that may be modified slightly in response to data as it is collected.



High Level Descriptions

Reconnaissance:

The initial phase of any security review involves extensive data collection. Penetration tests 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 queries
- Route and Subnet Identification
- Host Fingerprinting (IP scanning) and SNMP sweeps
- Network mapping with traceroute and other tools
- Social Engineering (if allowed)
- Wireless Testing (when in scope)
- War Dialing (when in scope)
- Initial target identification

Verification:

Once the Verification 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 in the first two stages. Methods of performing this phase can include:

- Vulnerability scanning
- Port scanning
- Alternate route & backdoors identification
- Identify exploitation targets

Exploitation:

The exploitation phase is typically only used when a client needs to demonstrate actual data or system compromises. 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. This methods used during this phase are tightly controlled by the penetration agreement and activities; highest consideration is always paid to avoid damaging or disrupting any customer computing resource or information. All activities are extensively logged.

Detailed Descriptions

Reconnaissance Details:

1. Reconnaissance

This phase involves the gathering of information about the client's network. Some attack methods may only apply to "insider" reviews. The methods employed include:

- Going to the Company Web Site (Internet or Intranet), and collecting information, such as location, phone number, systems employed, configuration information, etc.
- Performing Domain Name Server (DNS) lookups, or contacting InterNIC directly to obtain a list of IP addresses for the client, and possibly to gain information about the client's ISP.
- Using traceroute to help determine the structure and layout of the network.
- Using nslookup to identify authoritative and secondary DNS servers and to identify IP addresses between which zone transfers occur.
- Using traceroute to help determine the structure of the network.
- Social Engineering to gain information about the organization of the client, key personnel, important individuals (when in scope).
- Looking through public information about the company, annual reports, press releases, etc. (when in scope).
- "Dumpster Diving," gathering information by going through the client's garbage (when in scope).
- Using access to company directories and organizational charts to discover names, titles, and positions of employees for future exploit.
- Newsgroup reviews. Go to the major newsgroup archives and look for posting by client employees, or about client networks, products, etc.
- Using ping or another form of network scanning to detect those machines that are on the Internet and available from a given location and performing host fingerprinting.
- Operating System fingerprinting to help determine what OS a machine in the target network is running.
- Simple Network Management Protocol (SNMP) scanning to determine the machines that are running SNMP and if they have a strong or easily-guessed SNMP password.
- Wireless Testing, used to determine if Wireless LANs are vulnerable to attack (when in scope).
- War Dialing to determine if the client has modems listening on phone lines that may allow access to the network (when in scope).
- War Driving and similar methods to find unsecured or rogue access points (when in scope).
- Wireless Threat Assessments and similar methods. Used to find unsecured or rogue wireless access points.
- Initial target identification.

Verification Details:

2. Service Availability

This phase involves the service level information about the client. The methods employed include:

- Port Scanning, to gain a list of those services (Ports) that are available.
- Null Session connections and scanning (Windows Machines Only). This is used to determine the services available, lists of users, and other login information.
- Share Scanning to determine what shares machines have available.

- NetBIOS name and service scanning on Windows machines to determine services running.
- Utilize vulnerability testing tools (e.g.)¹
 - Nessus
 - Nmap
 - SAINT
- Identify alternate routes & backdoors
- Identify exploitation targets for the next phase

Exploitation Details:

The exploitation phase is typically used only when a client needs tangible evidence of actual data or system compromises. This phase involved exploiting identified vulnerabilities to gain access to internal systems, services, and networks. This phase typically utilizes many tools available in the public domain and used by attackers in real-life settings. To provide a more complete test, Emagined Security penetration testers also use proprietary (commercial) tools. In performing the System / Service exploit attempts, authentication attacks, and attempts to gain control of systems and internal networks, the following methods may be performed:

3. Avoid Detection

While avoiding detection is shown as its own phase, typically the testers will attempt to avoid detection during all phases of the penetration test. Activities testers may employ to avoid detection include:

- Using “Stealth Scans” to avoid detection.
- Deletion of System logs to eliminate a record of what was done on a machine.
- Disabling of logging functions on a particular machine while testing activities occur (typically left on to ensure full data is archived).
- “Selective” editing of log data to remove suspicious activity.
- Creation of scripts that generate large amounts of log “noise” to fill up logs, cause logs to reset, or obscure suspicious entries in the logs.
- Placement of hidden files/directories (possibly orphaned), backdoors, or Trojan Horse tools to hide the existence of files placed on the machine by the testers. (For example a “ls” command in Unix that does not show files located in a specific directory)

If any modification of client files (such as logs) is performed, it must be only with the client’s express written permission. Ideally, a client representative such as a system or network administrator will also be present when any modifications of files (e.g., system configuration files) must be made in according with testing procedures.

4. Acquire a User Account

This phase involves the acquisition of a working user account. The ultimate goal of any penetration test is to gain access to either root (in Unix systems), Domain Administrator in Windows systems, or Supervisor/Administrator in Novell NetWare systems. Using the information gained during the reconnaissance phase, our pen testers’ attacks are focused on machines running exploitable services. Methods we typically use include:

- Guessing passwords for accounts.

¹ Emagined Security routinely reviews and updates tools based upon industry standards and new technology advancements.

- Using automated password cracking tools to try large numbers of different potential passwords on a specific account.
- Using known exploits, including buffer overruns and format strings, to gain root/Administrator access.
- Using known exploits to gain access to the password file on a machine and then using “cracking” software to extract valid username and password combinations.
- Social Engineering to get users to reveal their username and password or other information canin order to facilitate a successful attack if the persons performing the test act as client employees or service providers.
- Shoulder surfing, or watching as other personnel login at their terminals.
- Harvesting passwords and encryption keys from the cache or memory pages of machines used in obtaining remote access to superuser accounts.
- Employing “sniffers” to watch traffic on the network and extract passwords and usernames. This also may include “hi-jacking” of telnet sessions. Techniques may also include capturing login information and replaying it later to login as that user.
- Tricking users to install Trojan horse software on their machines, enabling the testers to gain access later. (Loki, SubSeven, NetBus, Rootkit.Gen, Win32Beagle, and more)
- Installing Trojan horse software to capture keystrokes, passwords, or other information. (Keylogger, KeyCap, PassFilt.dll)
- Exploiting access granted to unauthenticated users (FTP, web browsing, registry) to gain access to sensitive files, such as the password file, or to expand existing access.
- Installation of an access point through some other means, such as creating new user accounts, placing back doors, or starting easily exploited services/ports.

5. Access Resource Over the Network

After a user account has been established on one machine, the testers then try to branch out and gain access to other information via the network. This can be as simple as stolen credentials to access Human Resource files (if the account belonged to an HR staff member). This phase of the test involves attempting to access sensitive data and information that the client wants to protect. This portion of the test should almost always have a client representative present to help ensure that testers are not blamed for accessing out of bounds material. Methods to perform this portion of the test include:

- Exploiting weak internal data access rules that allow regular user accounts to access what should be restricted data.
- Executing exploits available to users, such as registry exploits, installation of Trojan horses, etc.
- Using files found on one machine that may contain login or access information about other machines. (.rhosts, hosts, NIS maps, etc. on Unix and Linux machines.)
- After access is gained, the testers will typically create other methods for easy access. This may include creating new user accounts, placing back doors, or starting easily exploited services/ports.

6. Denial of Service (DoS)

This phase involves testing the network to see if it is susceptible to DoS attacks. Typically these attacks are used to deny service to either network resources or a particular machine. However, these attacks can be used as part of an effort to break in, especially if a trojan horse requiring a reboot of a machine has been installed. From a penetration test standpoint, the only testing for DoS attacks will center on whether the machines/systems being tested are vulnerable. Unlike the other phases of the penetration test, we will notify the IS staff before launching these attacks, and only attacks for which a patch is available are launched. For example, the client who wants to know if systems are vulnerable

to the Sockstress² attack on a Windows server would first apply the patch for the vulnerability. Emagined Security would then launch the attack to determine if the patch was successful in eliminating the exposure. DoS testing is typically done only during non-business hours. DoS testing should not be taken lightly, and should only be performed when the customer understands the risks and has individuals standing by during the test if a system, application, or the network becomes non-responsive.

7. Exploit Physical Access to Workstations/Servers

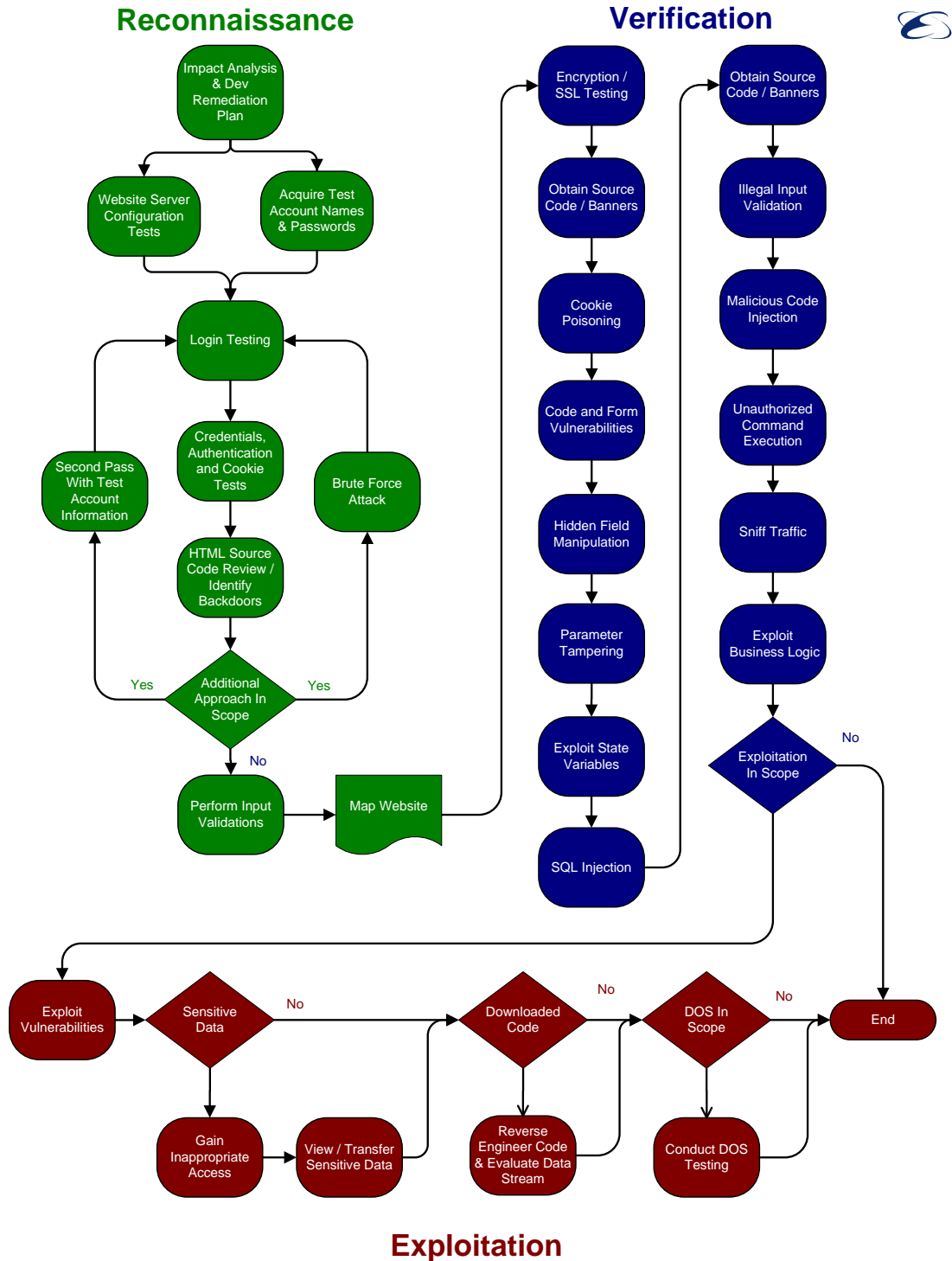
This phase is for internal tests only and uses exploits for physical access to the network/network computers. Tactics include:

- IP Spoofing to impersonate trusted machines.
- Sniffing network traffic to get additional passwords for more powerful users.
- Using boot disks to create accounts/change passwords for powerful accounts.
- Removal of hard drives for exploit at other locations.
- Removal of information in printouts by removing from premises.
- USB boot-keys, key loggers and attempts to have employees connect to insecure systems to download/exploit login scenarios.

² In a Sockstress attack an attacker attempts to exploit a vulnerability in the TCP/IP stack of Windows systems by sending an extremely large number of specially crafted packets in which the TCP receive window size is very small.

Phases of the Web Application Penetration Test

Penetration tests typically follow a structured approach that may be modified slightly in response to data as it is collected.



High Level Descriptions

Reconnaissance:

The Web Application Ethical Hack begins with Reconnaissance that can be designed to evade detection. Emagined Security tests each application's security controls to determine if an attack may result in inappropriate viewing, altering, copying or deleting information. During Reconnaissance, Emagined Security performs the testing activities mimicking two types of users:

- The unauthorized user attempting to gain access
- As an authorized user trying to acquire and utilize enhanced or inappropriate privileges

In addition the following is tested:

- Brute force authentication techniques, if authorized
- Perform credentials, authentication and cookie testing
- Review source code and identify backdoors
- Perform input validations
- Map website

Verification:

The assessment then moves into Verification where the majority of website manipulation takes place. Through our automated and manual process, Emagined Security reviews for many security risks. Emagined Security reviews for these risks by first performing system identification. Once Emagined Security has determined the operating system, web server versions and other associated systems, Emagined Security is able to quickly identify well-known system vulnerabilities. Emagined Security attempts to identify security risks resulting from weaknesses such as:

- Weak or no encryption / SSL vulnerabilities
- Obtain unprotected source code
- Cookie Poisoning
- Code & Form Vulnerabilities
- Hidden Field Manipulation
- Parameter Tampering
- Exploit state variables
- SQL Injection Issues
- Source code / banners
- Input validation errors
- Malicious Code or Command Injection
- Sniffable traffic
- Executable code vulnerabilities such as buffer overflow conditions and IIS weaknesses
- Identification and exploitation of Business Logic

Exploitation:

Finally, the assessment escalates to Exploitation where Emagined Security attempts to fully compromise the pre-agreed to target(s) (e.g., web infrastructures). Before Emagined Security begins any security assessments, Emagined Security works with the specified website owner to determine the ground rules for vulnerability exploitation.

Within the realm of Exploitations, Emagined Security performs services based on the type of website:

- The basic service includes identifying and exploiting the implemented security controls or lack of controls
- For applications with sensitive data, we attempt to gain unauthorized access and transfer data between test accounts and/or perform other transactions without providing appropriate target authentication
- For web applications that use downloadable code, we attempt to identify vulnerabilities associated with installing and operating the executable
- Perform a DoS attack on the websites included in the agreed upon scope of testing

Detailed Descriptions

Reconnaissance:

1. Testing Preparation

Emagined Security will start the project by assessing the impact of potential interruptions on the business's operations and business. Emagined Security will explain the ramifications of each identified potential interruption and inform the website owners of the processes necessary to reduce the risks from effects of conducting the testing. Emagined Security further performs scheduled and selective probes of the network's communication services, operating systems, key applications, and network equipment in search of those vulnerabilities. The following steps of the methodology will be completed:

- Prepare Impact Analysis & Remediation Plan
- Acquire Test Account Names & Passwords

Emagined Security typically requires the following information prior to starting testing:

- Network diagrams of the Internet Gateway Infrastructure
- IP address of the firewalls, DNS servers, routers, hubs, load balancers, supporting systems, as well as other network devices
- IP addresses of the associated internal systems
- Available documentation describing system process flows

2. Website Mapping

Emagined Security will test application security controls to determine if an attack may result in unauthorized viewing, altering, copying or deleting information. During Reconnaissance, Emagined Security will perform the testing activities mimicking two types of users:

- Unauthorized user attempting to gain access
- Authorized user trying to acquire and utilize enhanced or inappropriate privileges

During this part of the test, Emagined Security will attempt to gain access as an authenticated user to information not associated with that user. Emagined Security will also attempt to elevate user levels to privileged accounts or to other individual's accounts. Emagined Security will attempt to login to the system as various users and swap sessions or transfer sessions to another user. Emagined Security will also assess what happens when a user attempts an unauthorized transaction and when timeouts occur. Emagined Security will also attempt to evaluate how error-handling processing takes place when a user tries an unauthorized transaction. Emagined Security will accomplish this by conducting the following tests:

- Server and web server configuration updating and patching failures or weaknesses
- Login exposures due to weak credentials (e.g., easy-to-guess passwords)
- Credentials Authentication and Cookie Tests
- An HTML Source/Application Code Review, looking for back doors or debug option weaknesses
- Input validation including behavior to typical commands such as GET, POST, HEAD and PUT.

Examples of these tests include:

- Wherever there is a login prompt, Emagined Security will attempt to login using various names and passwords. Emagined Security will also attempt to guess usernames on well-known default and generic legacy accounts.
- Emagined Security will attempt to use “forgotten password” procedures, if they exist, to attempt to acquire information that could result in access.
- If there is a backend database, Emagined Security will attempt to acquire direct access, login and request information based on backend database passwords (especially well-known default passwords). Once Emagined Security has acquired access, Emagined Security will attempt to gain user information from the backend database.
- If in scope, Emagined Security will perform brute force username and password attacks.
- Emagined Security will search through html source code to attempt to identify hard coded names and passwords and identify backdoors that could be used to access backend database information without authorization. As described above, once we have gained access, we will attempt to acquire user information from the backend database.
- Perform input validation tests to identify issues with system client / server communication protection mechanisms.
- If within scope, Emagined Security will launch man-in-the-middle (MITM) attacks that could result in sniffing names and passwords if sessions are not SSL-protected.

During this phase, Emagined Security will also search through html source codes to attempt to identify hard coded information that could lead to identification of the associated web application scripts. Once Emagined Security has identified and acquired files with scripts, Emagined Security will attempt to analyze the business logic built in to Java, CGI, or PHP scripts used that would allow a user to exploit vulnerabilities in a web or database server. Emagined Security will also attempt to use any error checking or script documentation to our advantage in performing the assessment.

Verification:

3. Vulnerability Identification

The assessment then moves into Verification where the majority of website manipulation takes place. Through our automated and manual processes, Emagined Security will look thoroughly for a wide range of security risks. Emagined Security will try to identify these risks by first locating and identifying systems. Once Emagined Security has determined the type of operating system, version of web server, and other critical information concerning other systems, we are normally able to quickly discover well-known system vulnerabilities. Emagined Security will also assess security risk due to problems such as:

- Weak or no encryption / SSL vulnerabilities
- Obtain unprotected source code
- Cookie Poisoning
- Code & Form Vulnerabilities
- Hidden Field Manipulation
- Parameter Tampering
- Exploit state variables
- SQL Injection Issues
- Source code / banners
- Input validation errors
- Malicious Code or Command Injection
- Sniffable cleartext traffic
- Executable code vulnerabilities such as buffer overflow conditions and a variety of other web server bugs
- Exploitation of state information in URLs and cookies

- Identification and exploitation of Business Logic

Each part of this test has an associated, detailed methodology. For example, Emagined Security has a section entitled “Parameter Tampering.” In this portion of our methodology we test the effectiveness of an application’s error and exception handling capability. By using a smart proxy, Emagined Security can modify information after it has left the browser, but before it arrives at the server. This allows us to ensure that server-level validation is being performed and that the system does not entirely rely on client-side validation. For example, during this test, Emagined Security performs the following steps:

- Emagined Security also has the ability to compromise authorized users’ systems and set up a proxy that harvests unencrypted information, even though both the user and the system appear to have an SSL session. This method requires physical access to users’ systems and is typically out of scope.
- Verify that end users cannot send data to gain information from other persons, as in SQL injection attacks. Using this technique, Emagined Security may be able to run any SQL command on your database.
- Verify that vulnerabilities that allow unauthorized modification to data are identified and that access authorization is controlled by the system, not the end user.
- Review SQL transactions to ensure that data sent to the user is appropriate and that it does not include unnecessary data.
- Validate that each database sends proper responses based on rights and privileges assigned to each user.
- Identifying cross-site scripting vulnerabilities in which Emagined Security could use a script on a malicious web server to inject malicious code, steal cookies, and initiate other actions that could potentially compromise users’ systems.
- If in scope, attempt to corrupt SQL queries in a way that causes a database to crash or reveal information that should not be accessible.

Exploitation:

4. Exploit Identified Vulnerabilities

Before Emagined Security begins any security assessments, Emagined Security will work with the owner of each targeted website to determine appropriate ground rules for vulnerability exploitation. If Emagined Security identifies security vulnerabilities, Emagined Security will normally have two potential courses of action: 1) stop and report the potential existence of the vulnerability, or 2) fully exploit the vulnerability and determine the extent of potential compromise. Typically, if Emagined Security determines that the exploitation-related risk is high, Emagined Security will normally not attempt to exploit the vulnerability without advance, written approval from the system (or in other cases, data or application) owner. The owner should weigh the risks and benefits associated with the second option before giving approval to carry it out.

During the basic service, if approved, Emagined Security will attempt to defeat or bypass implemented security controls or exploit any lack of controls. Please note that doing this corresponds to the Exploit Vulnerabilities phase of our penetration testing methodology.

5. Web Application with Sensitive Data Exploitation

For web applications with sensitive data, we will attempt to gain inappropriate access and transfer data between test accounts and/or perform other transactions without providing appropriate target authentication. This is conducted during these phases of the methodology:

- Gain Inappropriate Access
- View Sensitive Data
- Transfer Sensitive Data (e.g. Financial)

In addition, Emagined Security will attempt to view sensitive and private information from test accounts by bypassing normal security controls. We will perform all of this type of testing from this type of account.

6. Downloadable Code Exploitations

For web applications that use downloadable code, Emagined Security will attempt to identify vulnerabilities associated with the installation and operation of the executable. This is conducted during the following phases of the methodology:

- Evaluate Installation & Authentication Process
- Reverse Engineer Code
- Evaluate Data Stream

During this stage, Emagined Security will attempt to identify vulnerabilities associated with the installation and operation of the executable. Specifically, Emagined Security will attempt to perform the following tests:

- For manually installed applications or downloaded applets, Emagined Security will attempt to evaluate the installation procedures and evaluate system modifications.
- Once applications or applets are installed, application processes will be evaluated to determine if any potential vulnerabilities may have been introduced. In addition, Emagined Security will assess the installed software components and configuration files to identify potential modification points that could be used to circumvent security controls.
- For Java applications, Emagined Security will attempt to reverse engineer downloaded software components. Emagined Security will analyze the generated source code to identify potential ways that the code can be manipulated. If successful in modification attempts, Emagined Security will attempt to recompile the code and use it to communicate with the application.
- Emagined Security will attempt to identify hard-coded values in applications and manipulate them in an effort to gain additional privileges and / or modify transactions. Modifications to the Windows registry will also be identified in an attempt to manipulate them for the same purpose.
- Data passed between the client and the web application will be captured and analyzed to identify potential vulnerabilities. Emagined Security will then attempt to manipulate and resend information to evaluate security controls. As feasible, Emagined Security will also attempt to modify the communications in real-time.
- The strength of the authentication process will also be tested to determine whether or not it can withstand typical exploits. As available, logout and timeout functions will also be conducted. In addition, Emagined Security will attempt to bypass any authentication mechanisms used by each tested application.

7. DoS Testing

This phase involves testing the website/application/system to see if it is susceptible to DoS attacks. Typically these attacks are used to deny service to either system resources or a particular machine. However, these attacks can be used as part of an effort to break in, especially if a trojan horse requiring a reboot of a machine has been installed. From a penetration test standpoint, the only testing for DoS attacks will center on whether the websites/systems being tested are vulnerable. DoS testing is typically done only during non-business hours. DoS testing should not be taken lightly, and should

only be performed when the customer understands the risks and has individuals standing by during the test if a system, application, or the network becomes non-responsive.