22-23 5G000

Statement of Work

Penetration Testing

Prepared
Martin Yarborou
Martin Yarborough and Associates

Table of Contents

Statement of Work for <<CUSTOMER<<

This Statement of Work (“SOW) is between Martin Yarborough & Associates (“Company”) and <<Customer>>(“Customer”) for the services described in the SOW (individually, the “Service” or collectively, the “Services”) and is effective as of the date last executed in the Signature section below.

Confidentiality: All information supplied to Customer for the purpose of this SOW is to be considered confidential.

Penetration Testing

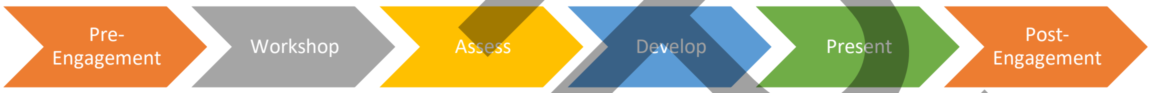
Overview and Shared Objectives

Customer has requested Martin Yarborough & Associates to provide a Statement of Work and pricing for the implementation of black box, external penetration testing (non-credentialed):

The objectives of the engagement are:

1. Conduct a workshop to review process, scope, safety and deliverables.
2. Conduct an NMAP review of 36 selected endpoints.
3. Conduct a Full/Deep vulnerability review of 36 selected endpoints.
4. Conduct a Metasploit review of 36 selected endpoints.
5. Conduct manual penetration testing of 36 selected endpoints.

Martin Yarborough & Associates executes such a program by implementing the engagement in a very structured manner:


Pre-Engagement
Workshop
Assess
Develop
Present
Post-Engagement

Project Scheduling

Martin Yarborough and Associates provides a high-level project plan as part of this SOW. A final plan is provided following the workshop phase of the engagement. A work-breakdown structure of a DRAFT plan is as follows:

Project Scope and Definition

Pre-Engagement

The engagement begins with the Pre-Engagement phase. Following the completion of all contract logistics with a signed SOW and purchase order, MYA will submit the pre-engagement worksheet to the procurement department for completion. This document is designed to obtain information needed for the completion of a formal project plan. Procurement will return the pre-engagement worksheet to MYA.

MYA will then setup 2 conference calls: Sponsor Orientation and SPOC orientation. Each call is designed to last only 1 hour. During that time, MYA will overview the project, discuss deliverables, identify participation and expectations and discuss the logistics of the engagement.

Following the Sponsor/SPOC orientation calls, MYA will complete a final project plan and submit the plan to the engagement Sponsor for approval. Once approved, the engagement will progress into the workshop phase.

Workshop

Once the project plan is approved, the engagement enters into the Workshop phase. The SPOC will setup a 1-hour call with a selected group of individuals collectively known as the Stakeholders. This group should include the Sponsor, SPOC, IT personnel with a security interest from the following genres: Systems, Networking, Applications, Security, Desktop Support and possibly some non-IT personnel as needed.

Once the group is identified, MYA will develop a 1-hour technical workshop to overview the engagement. Included will be:

- Introductions
- Review of Penetration Testing
- Project Management
- Safety and Security
- Discovery/Scoping
- Communication Plan
- Deliverables
- Q&A

MYA will conduct weekly status updates with the Sponsor and SPOC. Following the workshop, calendar invites for the needed status calls will be provided. Theses status calls are designed to provide the Sponsor/SPOC with a review of the previous week's work and an overview of the work to be performed during the following week. In addition, "Quick Hits" will be discussed. These are work efforts that should not wait until the end of the engagement. This time will also allow for socialization of the key findings.

Assess

Following the Workshop phase, MYA will implement the assessment portion of the engagement. The assessment will include black-box, external (non-credentialed) network penetration testing of 36 selected endpoints.

Coverage

Network penetration testing includes firewall configuration testing, including statefull analysis tests and common firewall bypass testing, IPS evasion, DNS attacks including zone transfer testing, switching and routing issues and other network related testing. For us, it also includes a full port scan and subsequent testing of all discovered services on any host that is identified as a testing target. Common services like SSH, SQL Server, MySQL and other database services, SMTP, FTP etc. are all included. Standard, well known web applications like Microsoft Outlook logon pages, standard administrative interfaces for firewalls, printers and other standard administrative web pages are also included and will receive black box testing if discovered. In fact, everything we discover during a port scan will receive testing.

Tools

The primary tools we use for network penetration tests are:

- Nmap
- GreenBone Security Manager CENO
- Metasploit Framework Scanner

- AMap
- Custom Perl Scripts

Methods and Sequence

Whois lookups. For External engagements the first step in the network testing methodology occurs before any testing begins. We perform whois and network lookups on all IP addresses and ranges and should there be any question about ownership of any of the systems, we bring it to your attention.

Port Scan Configuration. MYA runs our standard port scan battery of tests. This includes not one, but ten different port scans with different configurations.

Vulnerability Scans. MYA runs our standard vulnerability scanner configuration. Our network vulnerability scanners use a standard, customized configuration designed to avoid denial of service tests and unsafe memory corruption testing and is also configured to use low thread counts to avoid overwhelming target systems or network devices.

Metasploit Scans. Once the port scans and vulnerability scans have finished, our Metasploit scripts are executed. Among other things, we check for evidence of common firewall misconfiguration that can be indicated by differing responses from the various port scans. Sifting through the data quickly is the reason we use Perl. Firewall configuration is not the only thing we are looking for at this stage.

Amap Scans. All of the data related to footprinting is also organized, any unusual ports or unusual responses are flagged, known web ports are identified, and Amap is run on all of those ports. Suspect data is captured. Zone transfer tests at this time are conducted, if it is an external test, to check your DNS server configuration for any domain names we have logged, and that data is captured. We also capture and organize all of the output from the vulnerability scanner, prepare the data for a manual review.

Manual Testing. Once we have rolled up all of the data from the automated tools, we start the real work. MYA checks for any evidence of IPS activity. MYA repeats the process using increasingly stealthy tactics until we can confidently report that the IPS is effective, or report on full or partial success in evading it. Next, MYA examines the data for any anomalies that might indicate a problem in firewall configurations. This typically includes some false positives, which are reviewed. MYA notes of any identified vulnerabilities and sorts them into two buckets: (1) those that require further validation and (2)those that are reliable and need no further validation.

Finally, we look at everything that has been identified for further testing. In general, vulnerabilities will fall into three categories at this point:

- Vulnerabilities that were identified by automation and are reliable. A finding report is prepared, along with any validating evidence from the automated tool.
- Vulnerabilities that were identified by automation but are not reliable until validated. These are validated using whatever tools or methods are appropriate. Screen captures and other evidence is collected, and a finding report is created.
- Possible vulnerabilities or simple suspicions identified manually. These are all tested, one way or another, until we are convinced that we know what we are seeing and can either dismiss them or report them.

Develop

At-A-Glance

MYA develops a detailed database of all findings created during the assessment phase called the At-A-Glance. This tool is used to help identify potential impacts, risk and areas of concern. A detailed risk assessment (Red/Amber/Green) will be performed against all areas entered into the At-A-Glance and a maturity of each finding will be determined. This document is generated in a Microsoft Excel format in the entire document is provided as a deliverable.

Prepare Deliverable Templates

MYA prepares standard templates used to provide a Penetration Testing Executive Management Report, and a detailed Transformation blueprint to guide in the development of a mitigation plan as part of the primary deliverable package set.

Penetration Testing Executive Management Report

This document contains the following chapters:

- Executive Summary
- Remediation Guidance
- Recommendations
- Scope of Testing
- Methodology Summary
- Testing Details
- Penetration Testing Objectives
- Findings Detail

Vulnerability Review

This document contains the following information:

- IP
- Hostname
- Port
- Port Protocol
- CVSS
- Severity
- Solution Type
- NVT Name
- Summary
- Specific Result
- NVT OID
- CVEs
- Task ID
- Task Name
- Timestamp
- Result ID
- Impact
- Solution
- Affected Software/OS
- Vulnerability Insight
- Vulnerability Detection Method
- Product Detection Result
- BIDs
- CERTs
- Other References

Metasploit Review

This document contains the following information:

- Executive Summary
- Test Scope
- Results
- Recommendations

- Testing Approach
- Discovery and Reconnaissance
- Validation and Exploitation

Present

- MYA sets up and conducts a session with the Sponsor and SPOC to review all deliverable documents and address any questions/concerns raised as a result of the deliverable products.
- Following the Sponsor/SPOC review, MYA will assemble a mitigation plan to address issues identified during the review process and those issues to the Sponsor's approval.
- Once deliverable documents are in a final form, MYA works with the SPOC to establish a date/time for a full stakeholder review of the assessment deliverable products. This review requires one hour, and adequate time is provided for any questions from the group.

Post-Engagement

- Once the stakeholder review has been completed, MYA generates all deliverable documents in final form (electronic and print) and provides the documents to the sponsor through our electronic portal.
- The sponsor receives a short Customer Satisfaction Survey, completes and submits. Following the submission, MYA addresses any issues/concerns provides resolution to the Sponsor's satisfaction.
- Once issues identified in the Customer Satisfaction Survey have been addressed, MYA submits a final invoice and provides shippers to return the vulnerability scanner and the Metasploit scanner.
- Once the appliances have been received in-house, MYA closes the project.

Deliverables

Item	Description	Format
1	At-a-Glance Workbook	Excel
2	Penetration Testing Executive Management Report	PDF
3	Vulnerability Report	PDF
4	Metasploit Report	PDF
5	Transformational Blueprint	PDF
6		
7		

Assumptions and Customer Responsibilities

Assumptions:

The Company may make certain assumptions while specifying the Services and deliverables detailed in this SOW. It is the Customer's responsibility to identify any incorrect assumptions or take immediate action which will make all of the Company's responsibility to identify any incorrect assumptions or take immediate action which will make all of the Company's assumptions correct. Martin Yarborough & Associates has made the following specific assumptions while specifying the Services detailed in this SOW:

1. If the assumptions used to develop the SOW are found to be incorrect, the parties agree to meet and negotiate, in good faith, equitable changes to the SOW, Service Levels and/or Fee Schedule, as appropriate.
2. The prices for the Services are based on Customer's environment as known by the Company at the time of execution of this SOW. If the volumes, consumption factors or requirements change by plus or -5 (5%) percent, the county will adjust the pricing to reflect these changes.
3. The resources to perform the Services shall be available (including any travel time) Monday through Friday, 8:00 AM to 5:00 PM local Customer time (excluding nationally observed holidays, based on a forty (40) hour week, unless previously agreed upon between Customer and Company.

4. The Company reserves the right to perform portions of the work remotely according to a schedule mutually agreed to by both Customer and Company.
5. A typical schedule involves working remotely at least one business day per week to complete deliverables and/or any applicable documentation. Additional fees may apply for travel/Services outside of this timeframe.
6. This SOW includes travel to one domestic location(s) within the Continental United States as detailed in this SOW. Any additional travel to other locations is considered out of scope and will require the approval of Customer via the change control process detailed in this SOW.
7. The Company is not responsible for resolving compatibility or other issues that cannot be resolved by the manufacturer or for configuring hardware or software in contradiction to the settings supported by the manufacturer.
8. The Company is not responsible for project or Service delivery delays caused by Customer facility or personnel challenges.
9. Completing transition within the agreed timeframe is contingent upon the Company receiving the necessary Customer information and gaining access to the necessary Customer resources, personnel and facilities in a timely manner.
10. The Company's pricing does not assume the responsibility of any Customer or third-party personnel, hardware, software, equipment or other assets currently utilized in the Customer's operating environment.
11. The Company reserves the right to sub- contract portions of all of the requested Services with permission from the Customer.
12. The Company will not issue an intentional Denial of Service(DOS) or Dynamic Denial of Service(DDOS).

Not Included with This Service:

- Any services or activities other than those specifically noted in this SOW.

Customer Responsibilities

Both Customer and Company are responsible for collaborating on the execution of the Services. The Company's responsibilities have been set forth elsewhere in this SOW. Customer agrees generally to cooperate with Company to see that the Services are successfully completed. Customer agrees to the following assigned responsibilities:

1. Prior to the start of this SOW, Customer will indicate to Company in writing a person to be the single point of contact, according to the project plan, to ensure that all tasks can be completed within the specified time period. All Services communications will be addressed to such point of contact (the "Customer Contact"). Failure to do so might result in an increase in project hours and/or length in schedule.
2. Customer will provide technical points-of-contact, who have a working knowledge of the enterprise components to be considered during the Services ("Technical Contacts"). The Company may request that meetings be scheduled with Technical Contacts.
3. The Customer Contact will have the authority to act for the Customer in all aspects of the Service including bringing issues to the attention of the appropriate persons within Customer's organization and resolving conflict in requirements.
4. The Customer Contact will ensure that any communication between Customer and Company, including any scope-related questions or requests, are made through the appropriate Company Project Manager.
5. The Customer Contact will provide timely access to technical and business points of contact and required data/information for matters related to the scope of Service.
6. The Customer Contact will ensure attendance by key Customer contacts at Customer meetings and deliverable presentations.
7. The Customer Contact will obtain and provide project requirements, information, data, decisions and approvals within one working day of the request, unless both parties agree to a different response time.
8. Customer may be responsible for developing or providing documentation, materials and assistance to Company and agrees to do so in a timely manner. Company shall not be responsible for any delays in completing its assigned tasks to the extent that they result from Customer's failure to provide such timely documentation, materials and assistance.
9. The Customer Contact will ensure the Services personnel have reasonable and safe access to the Project site, a safe working environment, an adequate office space, and parking as required.
10. Customer will inform Company of all access issues and security measures and provide access to all necessary hardware and facilities.
11. Customer must indicate that they own each of the IP endpoints to be tested. (Verified with Whois)
12. Customer must divulge if the penetration testing results will be used to satisfy any compliancy issues.
13. Customer must divulge if any of the endpoints to be tested contain:
    a. ActiveX Controls

   b. Silverlight Controls
   c. Java Applets
   d. Web Service

14. Customer must divulge if the endpoints have undergone penetration testing within the past 2 years.

Change control process

- The “Change Control Process” is the process that governs changes to the scope of the Services during the term of this SOW. The Change Control Process will apply to new Services components and to enhancements of existing services.
- A written “Change Order” will be the vehicle for communicating any desired changes to the Services. It will describe the proposed changes to the Services scope, pricing, resources, tasks, and deliverables; the reason for the change; related assumptions and Customer responsibilities; and the schedule and price impacts of the change. The Company Project Manager will draft the Change Order document based on discussions with Customer and Company team. Only changes included in a Change Order signed by both Customer and Company will be implemented.
- In some cases, a Change Order will authorize Company to study the impacts of proposed change will have in terms of required changes to Services scope, schedule, and price. If, upon completion of the study, Customer agrees to proceed with an identified scope change, the Company Project Manager will draft a separate Change Order to detail the specifics associated with that change.

Martin Yarborough & Associates Personnel Skills and Qualifications

□ The Company, will, at its sole discretion, determine the number of personnel and the appropriate skill sets necessary to complete the Services.

□ Customer understands that Company resources may include employees of Company and/or a service provider or subcontractor to Company.

□ Company personnel may work on-site at Customer location or off-site inside at a Company or other location as determined by the needs of the Services and by specific agreement of the Customer project manager.

□ Company has identified the following initial resource levels for these Services. Key responsibilities for the resources are identified below.

Martin Yarborough

Career Summary

For three decades Martin Yarborough has been involved in public education as a teacher, Director of Technology, Dean of Technology, Chief Technology Officer, and lastly, as the Chief Information Officer of the Fort Worth Independent School District, the fourth largest school district in Texas. This life-long Texan and seasoned educational professional received his Masters’ degrees in Educational Administration and Curriculum and Instruction from Tarleton State University in Stephenville Texas and Bachelors’ degrees in Chemistry and Biology from the same institution with doctoral work in Instructional Technology from the University of North Texas and Northern Illinois University.

Recognizing the potential of technology as a teaching and learning tool, Mr. Yarborough brought the Glen Rose public schools into educational technology prominence in 1982 by implementing the very first district-wide fiber-optic LAN in Texas, thus beginning a life-long love affair with educational technology that exists to this day. An innovator in implementing cutting edge, efficient technology into schools, Martin was among the first to implement voice over IP into classrooms, provide teachers with corporate-style email, develop a project-management practice to oversee large-scale, district-wide technology implementations, and incorporate extensive use of distance learning and professional development into public school classrooms.

His experience extends into application software development as well as management of large implementations of PeopleSoft, Computer Associates, and Microsoft deployments to include ERP products, network monitoring tools, email systems, K-12 ERATE, and portal environments. Martin was instrumental in the establishment of a comprehensive data warehouse and longitudinal data system for the Fort Worth public schools incorporating all benchmark and other testing data with student demographics in a SharePoint environment for access by faculty and staff through portal technologies.

Mr. Yarborough is a sought-after speaker on topics ranging from better efficiencies through assessments and educational practices as well as cybersecurity and disaster recovery.

Areas of Expertise

- **End User Computing** and client deployment strategies to include workstation management, output devices, and messaging practices (e-mail, instant messaging, voicemail, and fax).
- **Data Center Analysis and Design** to include server and server platforms including virtualization, storage (SAN, NAS and DAS), facilities management, backup/restore practices, and disaster recovery.
- **Application Enablement** to include business ERP, enterprise application software, software development lifecycles.
- **Security and Vulnerability** to include intrusion detection, account management and security assessments including penetration testing.
- **Services Management** to include service desk operation, change management practices, release management practices, problem management, and incident management. **Specialist in Business Impact Studies, Risk Analysis and Disaster/Recovery Planning.**

Project Experience

- **Medium City Government –** Conducted an IT Assessment and facilitated a strategic plan to expand the IT program to accommodate a large sporting event venue to be constructed within the city limits.
- **Large Professional Organization in California –** Facilitated a state-wide strategic plan for a large organization of IT professionals
- **Large Educational Service Center in California -** Served as Senior Consultant in the Disaster/Recovery planning development. The 6 week engagement resulted in a comprehensive metric identification practice through the evaluation of a Business Impact Analysis, Risk Assessment and Application Analysis. The evaluation led to the implementation of a Disaster/Recovery program for the organization to span 16 weeks.
- **Medium Utility District in Florida -** Served as Senior Consultant in the Disaster/Recovery planning development. The 8 week engagement resulted in the development of 8 application recovery plans, a server recovery program, a network recovery plan and a telecommunication program.
- **Medium Univerity in Texas –** Served as Senior Consultant in the Disaster/Revovery planning development. The 6 week engagement resulted in a comprehensive metric identification practice through the evaluation of a Business Impact Analysis, Risk Assessment and Application Analysis. The evaluation led to the development of an Educational Contingency Plan as well as a DR/BC plan for the college.
- **Large public school district in Virginia** – Served as project manager on an enterprise assessment making 15 actionable recommendations which resulted in a complete re-design of the service desk environment and desktop support. Six transformational follow-on engagements ensued.
- **Large public transportation company in South** – Served as Project Directory on an assessment to review plans for a secondary disaster/recovery site for the largest roadway project in Texas. The results were detailed recommendations for implementing a self-contained data center that could temporarily be located in a remote location and moved in the event of a disaster. The assessment engagement led to data center consolidation and transformation opportunities.
- **Large public school district in South** – Provided project leadership on the largest assessment to date of the second largest school district in Texas. The new CIO was struggling making decisions and putting business cases together to request additional budget. A complex, custom assessment was developed with intent to review budget, hardware and services in preparation for an ITO proposal. The result was praised by the CIO, CFO and Superintendent and the adoption of the assessment by the School Board serving as the basis for an on-going strategic planning effort.
- **Medium school district in the Heartland** – Worked with the superintendent of schools to conduct an extensive Educational Assessment. Results included recommendations to move ERP, Messaging and Network Services to a cloud delivered model. The district retained my services for a 24-month period to assist the organization in implementing the recommendations. I established a comprehensive PMO Framework and trained the staff on project management during the implementation. The result was a complete data center transformation. This was an acquisition account for my company and as a result of the relationships I established, they have been one of the highlights of this past year. The organization was selected as a case study. This included the pm of a GroupWise/Exchange migration, conversion from Novell to MS Active Directory, implementation of video conferencing as well as several staff augmentations using 3rd party vendors to assist in the implementation of an extensive wireless network.
- **Medium school district in the Heartland** – Conducted a 4 week assessment of the IT Enterprise to include end-user computing, services management, data center operations and security and vulnerability. Identified 15 core initiatives and

provided an operational roadmap for remediation. The result was an 18-month staff-augmentation as the interim CIO engaged to implement the suggested

- initiatives. The first step was the development of a PMO framework and staff training to implement the PMO.
- **State Government** – Conducted an enterprise technology assessment focusing on Administrative Applications, Web Operations and IT Infrastructure and Operations. Identified 12 core initiatives for transformation and submitted statements of work to deliver the transformational consulting. This included extensive leadership augmentation.
- **Large school district in South** – Fort Worth Texas – Provided the leadership to conduct an evaluation of ERP and Student Information Systems for transformation of the accounting practices of the district. Supervised the bidding and procurement process for the business ERP environment and let the implementation and migration practice for the successful implementation of Tyler Technologies MUNIS program.
- **Large school district in South** – Served in an interim CIO capacity to project manage a “botched” PeopleSoft implementation. I was able to bring the payroll system into compliance in less than 3 months and implement the benefit system.
- **Large school district in South** – Served as project manager for the conversion of a legacy ERP to a full PeopleSoft implementation. This involved the hiring of technical/functional consultants, procurement of equipment including bidding and supervising staff during this phase. The effort resulted in a successful implementation in less than 6 months of Financials/HR/Benefits and Payroll including self-service.
- **Large municipal government in South** – Conducted an enterprise technology infrastructure assessment. Engagement spanned 12 weeks of effort. Identified 14 core initiatives for improvement. Developed extensive roadmap for implementation. Follow-on included the implementation of a full-scale PMO and the training of staff to utilize the PMO framework as well as Novel⍰Microsoft conversions and data center transformations.
- **Large school district in West** – Evaluated infrastructure capacity leading toward 15 week engagement for an enterprise technology infrastructure assessment. Worked with technology staff to identify 12 primary initiatives toward improvement of core infrastructure to include end user management, service management, data center operations and security. Effort resulted in a storage transformation and key network transformations.
- **Large school district in South** – Worked with Superintendent and CIO to implement a comprehensive infrastructure assessment. Effort spanned 15 weeks and resulted in the development of 15 core initiatives focusing on data center, end-user and service management.
- **Large University in South** – Conducted a readiness assessment of classroom multimedia infrastructure. Effort resulted in an organizational re-design and re-organization to consolidate siloed IT programs into a centralized IT department and let to extensive consulting engagements post-ITSA.
- **Large University in West** – Conducted an enterprise technology assessment focusing on Administrative Applications, Web Operations and IT Infrastructure and Operations. Identified 15 core initiatives for transformation and submitted statements of work to deliver the transformational consulting. This included extensive leadership augmentations, ITIL training and data center transformation.
- **Medium University in South** – Served as project manager on an ERP/Student Information conversion from a legacy mainframe system to a Unix platform running on Alpha processors. Conversion took 4 months plus another 3 months to convert over 1MM transcript records into the new format. Conducted University-wide staff development to faculty and staff on the use of the new ERP/SIS environment and established process and procedure for the management of the system.

Professional Qualifications

Education

- B.S. Biology, Tarleton State University, 1979
- B.S. Chemistry, Tarleton State University, 1979
- M.Ed. Education Administration, Tarleton State University, 1990.
- Ph.D Instructional Technology, Northern Illinois University, 2001

Certifications

- Lifetime Teaching Certificate, Texas, 1979
- Mid-Management Administrative Certificate, Texas, 1990
- Superintendent Certificate, Texas, 1990

- PMP, 2007
- ITIL v.3, 2008
- TOGAF v.9, 2011
- Certified Ethical Hacker, 2015

Presentations and Publications

- T.H.E. Journal Publication – Author… "A Journey Across the Fiber", 1984.
- Educause Presentation – Speaker …"Assessment for Efficiency", 2008.
- ISTE Presentation – Keynote… "Designing a Better Educational Data Center", 1996.
- TechSig Presentation – Keynote… "Outsourcing Data Center Practices", 1992.
- SETL Presentation – Keynote… "Why Assessments Work", 2010.
- ATLE Presentation – Keynote…"How to Increase Efficiency in your Data Center", 2011.
- ASCD Presentation – Speaker…"Integrating classroom computers into the curriculum", 1996.
- MISA Presentation – Keynote…"Creating a climate of Efficiency in the Data Center", 2013.
- SETL Presentation – Facilitator … "Cloud Computing and BYOD", 2013

Termination

Customer may terminate this SOW for convenience upon providing Company with thirty (30) days written notice. Upon any termination of this SOW or the associated Agreement, Customer shall pay all of Company's unpaid fees and out-of-pocket expenses accrued to the effective date of such termination. If Customer fails to perform any payment obligations hereunder and such failure remains un-remediated for fifteen (15) days, Company may suspend its performance until payment is received or terminate this SOW and the associated Agreement upon written notice.

Pricing

Pricing for this engagement is set as Fixed Fee. It is estimated that the engagement will require 488 hours(app. 20 days) with 75 hours of billable consulting at a cost of $135/hr (inclusive of any travel or expenses). Due to the pandemic, travel is discouraged. A quote is provided at the end of this proposal.

Signature and Acceptance

By signature below, Customer and Martin Yarborough and Associates acknowledge and agree to this statement of work (SOW).

Client Contact Signature	*Martin Yarborough and Associates Contact Signature*
Printed Name	Martin Yarborough *Printed Name*
Title	Principal Consultant *Title*
Company Name	Martin Yarborough and Associates LLC *Company Name*
Date	May 26, 2022 *Date*

Please fax a copy of your Purchase Order and this signed SOW (with all pages in full) to 1-817-887-3371.

Quote

An itemized quote follows …

Martin Yarborough
and Associates

Quote

FROM:

Martin Yarborough & Associates LLC
8451 Deerwood Forest Drive
Fort Worth, TX 76126

TO:

Customer Name
Customer Contact
Customer Address
Customer City   Customer State Zip

Quote Number		**XXXXX**
Quote Date		**XXXXX**
Quote Total	**$**	**300.00**

Quant	Unit	Description	Cost		Amount
1	ea	Penetration Test per endpoint as per SOW	$ 360.00		$ 360.00
0	0	0	$ -		$ -
0	0	0	$ -		$ -
0	0	0	$ -		$ -
0	0	0	$ -		$ -

Net Total	$	360.00
Discount		GoodBuy
Tax		Exempt
Total Amount	$	300.00

Note: GoodBuy Contract 22-23 5G000

Payment Details		Other Information
Name of Benficiary:	Martin Yarborough and Associates	Martin Yarborough
Name of Bank:		(817)241-4777
Address of Bank:	Available upon request or on-file	Fax: (817)887-3371
Account #:		Email: myarb@martinyarborough.com
Routing #:		

Payment should be made by bank transfer or check made payable to Martin Yarborough and Associates

Martin Yarborough and Associates thank you for your business and prompt payment !!!