CyberOne

SECURITY ASSESSMENT

4/5/2024

Statement of Work (DIR-CPO-4851)

Security Assessment for City of Tomball by CyberOne, LLC.

Security Assessment

STATEMENT OF WORK (DIR-CPO-4851)

Table of Contents

EXECUTIVE SUMMARY

CyberOne, LLC. (CyberOne) is pleased to present this proposal for an Internal and External Penetration Test for City of Tomball ("Client" or "Customer"). The threat landscape is changing where personal information of customers and employees is a key target of hackers. The assessment will focus on the attack methods commonly used by malicious actors to gain access to customer and employee data.

This project is performed to identify vulnerabilities which an attacker may use to breach the network. This simulated multi-layered attack is performed on your organization to measure how well your people, processes, facilities, and technologies can withstand a real-life attack situation.

ABOUT CYBERONE

CyberOne is a Plano, TX based security company that is majority employee-owned with the goal to cost-effectively improve the security and compliance management capabilities of our customers by leveraging deep industry subject matter expertise. While focused on security and compliance services, we also resell a limited set of security products, and assist organizations that are moving from a reactive security to proactive security model, or who are working to address security and compliance challenges.

Our professional services teams provide a compliment of offerings to assist organizations with the development, maintenance, and assessment of Information Security, Risk, and Compliance Management Programs. Our teams of security analysts, assessors, and engineers deliver top tier real-world expertise regarding building and maintaining world class information security capabilities and governance programs, and have helped numerous organizations in the following markets achieve their security and compliance objectives:

- Retail and E-Commerce
- Banking and Financial Services
- Healthcare and Clinical Services
- State and Local Government
- Public Service and Transportation Organizations
- Technology Products and Services
- Manufacturing and Distribution
- Utilities and Critical Infrastructure

CyberOne also has an in-house research offensive and defensive team – TEAMARES – that focuses on investigating new threats and potential vulnerabilities industry-wide to protect our customers and partners. TEAMARES is also a premiere provider of all offensive and defensive security services including:

- Penetration Testing
- Web and Mobile Application Testing
- Full Red Team Engagements
- Password Quality Assessments
- SCADA and IoT Penetration Testing
- Incident Response
- Endpoint Digital Forensics
- Malware Reverse Engineering

ASSESSMENT ACTIVITIES

This assessment will simulate an advanced hacking team who is using multiple methods to obtain access into the Client network. During the assessment, a standardized methodology and framework called the MITRE ATT&CK is utilized to maintain a consistent approach to the testing. The use and understanding of this standard provide consistency, targeting specific compliance requirements, the ability to reproduce similar assessments in the future, and a consistent reporting approach.

CyberOne will perform an assessment based on the assessment requirements as understood by CyberOne. However, the MITRE ATT&CK methodology will be adapted to meet the Client's individual needs. CyberOne will attempt to exploit identified vulnerabilities to obtain a foothold into the environment. All exploitation methods will seek to disrupt, circumvent, or otherwise defeat the confidentiality, availability, or integrity of the Customer's environment. This may include using widely known exploits or workarounds unique to the Customer's environment. To fully understand the vulnerability profile of the environment, multiple scanners and scanning techniques will be used to uncover the full array of vulnerabilities. A large amount of the vulnerability discovery process will also be performed manually. This adaptation will be applied through the following phases requested by the Client:

Penetration Testing

- External Penetration Testing
  - Perform Foot printing and Reconnaissance Activities for Client
  - Manual scanning of identified network ranges
  - Performance of manual and automated checks for vulnerabilities,
  - Manually validate vulnerabilities
  - Web application attacks (unauthenticated) to identify vulnerable systems
  - Engagement goals:
    - Decreased external exposure.
    - Increasing user and management security awareness.
    - Gain insights into security posture.
    - Gap analysis
  - Scope Includes:
    - Approximately 10 live hosts
- Internal Penetration Testing
  - Perform Footprint and Reconnaissance internally.
  - Simulate an attack who has already gained access to internal network or an insider threat.
  - Utilize common hacking tools and techniques to enumerate trusts, common passwords, and privileged accounts.
  - Engagement goals:
    - Decreased external exposure.
    - Increasing user and management security awareness.
    - Gain insights into security posture.
    - Gap analysis
  - Scope Includes:
    - Approximately 240 live hosts

DOCUMENTATION

Using previous penetration testing experience, knowledge of current attacks, and our internal knowledge database, CyberOne will analyze the results of the assessment and validate findings to provide meaningful results that will enable the Customer to get to the root cause of the discovered vulnerabilities.

Our report will include an executive summary, high-level recommendations for remediation, and a detailed technical findings section. The executive summary section will reiterate the scope and purpose of the project and a list of key findings discovered during the assessment. A brief synopsis of remediation recommendations will follow the executive summary, which serves to highlight steps the Client can take to mitigate risk. The technical findings section will be compiled into a matrix by finding and each finding will include information regarding risk severity level, systems impacted, description of finding, business risk summary, recommendations for remediation and remediation effort level.

Project Documentation includes a combined report including:

- Executive Level Summary of Findings and Recommendations.
- Review of the work performed according to ISACA auditing standards.
- A quantitative overall risk score based on the average and impact of discovered vulnerabilities.
- Managerial level results from the penetration assessment which includes a narrative walkthrough of the steps performed based on the project timeline.
- Technical Findings of identified vulnerabilities, risk level, remediation effort and recommendations for correction.
- Executive Presentation of Findings.
- A post-assessment debrief with the ability to review the results of the assessment with the assessment team, ask detailed questions, understand strategic remediation guidance and engage in discussions as needed.

PROJECT MANAGEMENT

CyberOne will designate a project manager to oversee the project, manage CyberOne resources, and be the Customer's primary contact with CyberOne regarding the following:

- Management of scope (formal or informal requests for changes)
- Conducting Status Meetings
- Preparing Status Reports
- Other activities as specified in this Statement of Work

Additionally, project escalation and quality assurance resources will be designated to ensure that the Client receives the highest quality of service.

CHANGE PROCESS

The general change process will be implemented as illustrated in the Figure below. Either CyberOne or the Customer may initiate a change, in writing, to the Project. The change will be evaluated, and any Project impact will be identified. If the evaluation of a change request submitted by the Customer takes in excess of four (4) hours to complete, the cost of evaluation may be charged to Customer and any schedule slippage as a result of performing the evaluation will be documented as a formal change to the schedule. The price, scope, and schedule impact, if any, will be analyzed and documented. The change impact will then be processed for the Customer authorization or closure.

The change request form will include a description of the change, reason for it, and the initiator as well as the impact to the scope, price, quality, schedule, resources, and risks. All changes must be mutually agreed on by the parties in writing. Once approved, changes to the initial project will be implemented as described.

If CyberOne and the Customer are unable to resolve the disposition of the change order, the Project SOW will remain as defined in this document.

ESCALATION PROCESS

Timely resolution of issues is critical to maintaining project control and customer satisfaction. The purpose of the escalation process is to help ensure that issues are identified and resolved quickly. The escalation process provides a mechanism to alert the Project Managers and other management personnel to issues not being resolved. Either CyberOne or the Customer may escalate a project issue as follows:

1. Raise the issue initially to the CyberOne Project Manager or Project Lead.
2. If not resolved at this level, an issue report will be generated, and the issue will be escalated to the Project Sponsor.
3. Certain internal CyberOne issues may need to be escalated to the CyberOne VP or Managing Partner for resolution.

PROJECT RESPONSIBILITIES & ASSUMPTIONS

This section details the assumptions and high-level responsibilities associated with the delivery of this Statement of Work.

CLIENT RESPONSIBILITIES

- Assign a Project Sponsor who:
  - Is available to CyberOne personnel throughout the life of the project.
  - Acts as an escalation point when conflicts cannot be resolved by the Project Manager.
- Assign a Project Manager who is:
  - Responsible for all the Client aspects of this Project.
  - Authorized to make all decisions relative to the Project, including identification and assignment of the Client resources.
  - Available to CyberOne consulting personnel throughout the Project's life.
  - Is authorized to sign the Status Reports, approve consultant hours, and approve project changes.
  - Responsible for coordinating all interviews, onsite reviews, and meeting schedules.
  - Authorized to approve Project changes.
- Complete any documentation requests associated with this statement of work in a timely fashion and provide requested information to CyberOne project lead.
- Assign managers, process owners, and other personnel, as appropriate, to work with CyberOne throughout the project's life. The Client is expected to engage and participate throughout the project lifecycle phases. Project performance is predicated on the Client's staff, and response to documentation and information requests. Delays in providing this staffing or information may lead to a Change Order, and result in additional cost and/or delay in completion of the Services.

CYBERONE RESPONSIBILITIES

In addition to the Services defined throughout this SOW, CyberOne shall:

- Provide a single point of contact to the Client for the duration of the project for coordination and scheduling of project tasks, documentation, and any changes to scope requiring a change order.
- Coordinate activities of all CyberOne resources and provide the Client with a calling tree.
- Provide notification prior to the start of intrusive testing along with source IP addresses/ranges.
- Stop performing testing if degradation is identified on applications and networks being reviewed.
- Provide immediate notification if critical vulnerabilities are identified.
- Provide project documentation within an agreed upon timeframe, based on timelines and milestones defined at project kick-off.
- CyberOne resources may work remotely for portions of this engagement which do not require an on-site presence.
- Provide a single round of retesting services to validate remediation of vulnerabilities identified during the project within 90 calendar days from the delivery of the initial report.
  - Any additional Customer retesting requests will be considered on a case-by-case basis and may incur additional expenses.

- All retesting services must be scheduled at least 10 business days in advance to ensure resource availability.

GENERAL ASSUMPTIONS

- The Client will make reasonable efforts in advance of CyberOne's project activities to assemble all documentation and work papers within scope as identified by CyberOne.
- Any formal reporting of individual controls performed as part of ad-hoc testing will reference specific components which were evaluated and will not be construed to apply universally to all controls, environments, or components which may be applicable but were not evaluated as part of individual testing.
- The Client acknowledges and agrees that: (i) any outcome of the services involving compliance assessment is limited to a point-in-time examination of the Client's compliance or non-compliance status with the applicable standards or industry best practices set forth in the Scope of Work and that the outcome of any audits, assessments or testing by, and the opinions, advice, recommendations and/or certification of CyberOne do not constitute any form of representation, warranty or guarantee that the Client systems are 100% secure from every form of attack, and (ii) in assisting in the examination of the Client's compliance or non-compliance status, CyberOne relies upon accurate, authentic and complete information provided by the Client as well as the use of certain sampling techniques.
- Customer understands that CyberOne will take every possible precaution to safeguard against incidental interruption of Customer's environment. If an interruption is caused through accidental or unavoidable means, CyberOne will immediately notify Customer.
- By the nature of any network assessment process, CyberOne may be required to test the Customer's network. By signing this Agreement, Customer gives CyberOne permission to mimic unauthorized personnel and use intrusion methodologies that attempt to gain access to Customer's systems according to any subsequent Statement of Work supporting such a service. Customer is permitting CyberOne to attack the network as defined in any associated Statement of Work.

ORDER AND PAYMENT INFORMATION

CyberOne proposes to provide the Services and Deliverables at a fixed price not including travel expenses.

Table 1. Combined Project Cost

Type	SKU	Description	Combined Cost
Consulting	C1-PROSRV-TA-RED-NONR	External Penetration Test	$5,700
Consulting	C1-PROSRV-TA-RED-NONR-AL	Internal Penetration Test	$11,400
		Total Package Price USD	**$17,100**

Payment Terms

CyberOne will invoice the Client for half of the assessment (50%) at the project kickoff and the remaining amount and expenses at the delivery of the engagement report. All CyberOne invoices are payable NET 30 days.

Expenses

This assessment will be performed remotely, and no travel expenses or licensing fees are required. Any incidentals (e.g. shipping hardware) will be discussed with and approved by the client in advance and will be expensed at cost. If the Customer requests services that require travel, such as in-person debriefs or presentations outside of the DFW area, travel and incidentals will be billed in addition to the quoted package price.

Billing Contact:

City of Tomball	
Contact Name:	Tom Wilson Director of IT Security (281) 290-1405 twilson@tombaltx.gov
CyberOne	
Address: **City, State, Zip (Country):**	6851 Communications Parkway Plano, TX 75024
Senior Account Manager: **Phone No.:** **E-mail:**	James Bryant 469.562.8842 james.bryant@cyberonesecurity.com
Professional Services Project Manager: **Mobile No.:** **E-mail:**	TBD pmo@cyberonesecurity.com
Prepared By: **SOW Number:** **Issuance Date:** **Version:**	Andrew Johnson 28827 April 5, 2024 1.0

AUTHORIZATION

Agreement

In addition to the Client's execution of this SOW, CyberOne shall require a valid acceptable purchase order referencing this SOW in order to begin to provide the Services hereunder and the signature represents that their execution of this SOW is a binding commitment to purchase the Services described herein. However, in the event that the Client does not issue purchase orders as a matter of business practice, the Client herby warrants and represents that: i) its signature on this SOW authorizes CyberOne to provide the Services hereunder, and ii) that the Client shall pay for Services provided to the Client without the necessity of a purchase order, and iii) the Client will not contest payment for the provision of Services hereunder due to the fact that no purchase order was issued. Professional Services Terms and Conditions are addressed within the DIR CPO 4851 contract.

This SOW is valid for 60-days after issue date.

Effective Date:

City of Tomball	**CyberOne, LLC.**
_____	_____
Authorized Signature	*Authorized Signature*
_____	_____
Printed Name	*Printed Name*
_____	_____
Title	*Title*
_____	_____
Date	*Date*

Please email your documents to:

CyberOne, LLC.

ATTN: Sales Operations

Phone: 214.810.6760

Email: operations@cyberonesecurity.com