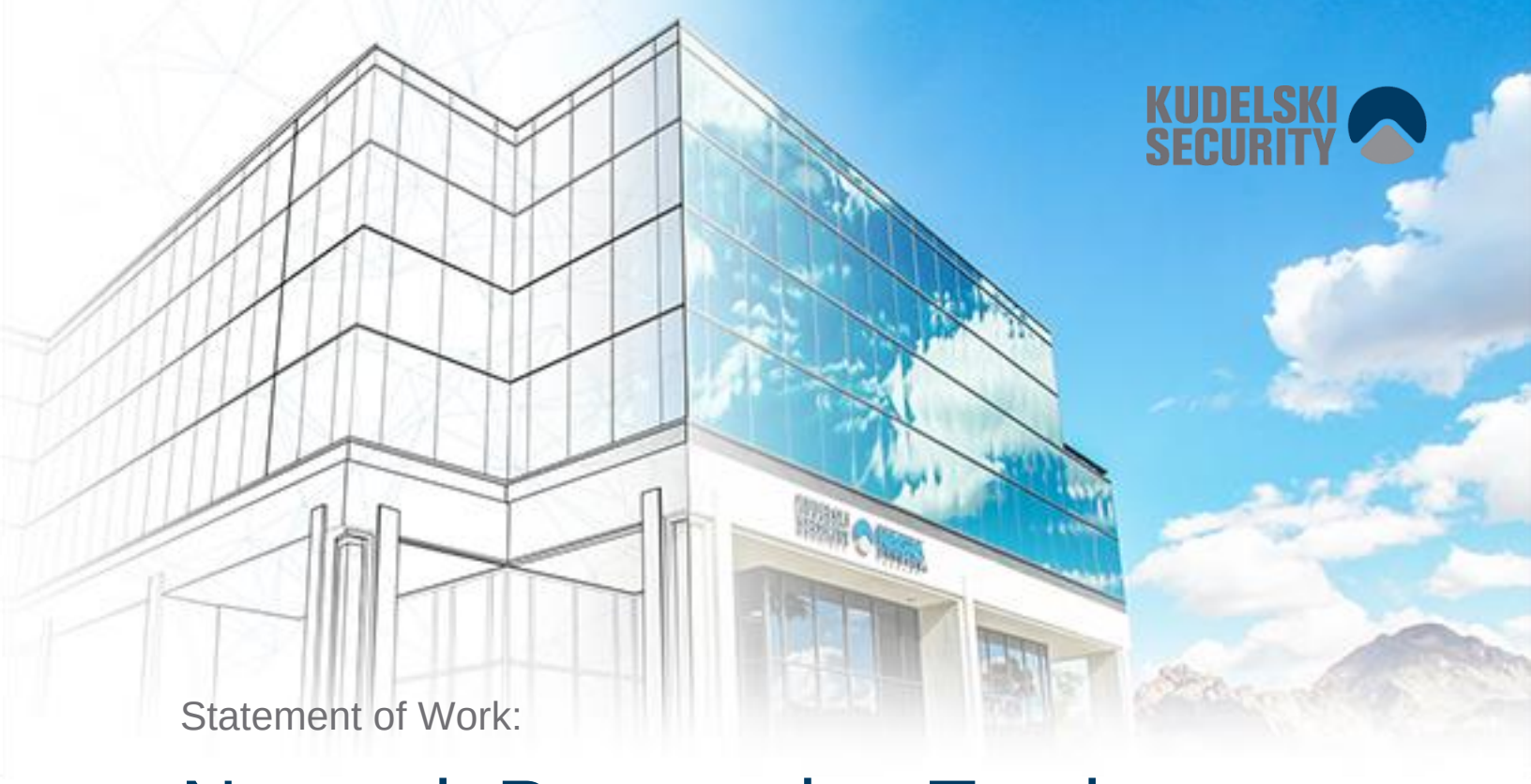


Statement of Work:

Network Penetration Testing

Prepared for:

City of Galveston, Texas

November 30, 2023
Version: 2.0
REQ3647 | OP049528

Presented by:

Matt Davis, Regional Sales Manager
Kudelski Security, Inc.

Corporate Headquarters
5090 North 40th Street, Suite 450
Phoenix, Arizona 85018

TABLE OF CONTENTS

STATEMENT OF WORK

This Statement of Work ("**SOW**") is entered into between Kudelski Security, Inc. ("**Kudelski Security**") and City of Galveston, Texas ("**Client**"), having a primary place of business at 823 Rosenberg, Galveston, TX 77550 (collectively, the "**Parties**"). This SOW shall be governed by the terms and conditions of the State of Texas DIR contract #DIR-CPO-4891. This SOW is effective as of the last date of signature herein ("**Effective Date**").

EXECUTION

Project Summary	The engagement is designed to identify complex vulnerabilities or exposed sensitive information that would not be detected by rudimentary penetration testing or vulnerability scanning. Testing will also uncover system misconfigurations and gaps within the Client's overall security posture which a skilled threat actor could leverage. Kudelski Security will conduct this comprehensive assessment remotely with Kudelski Security provided hardware or virtual appliances. Kudelski Security will also employ the use of custom tools and techniques during this effort.

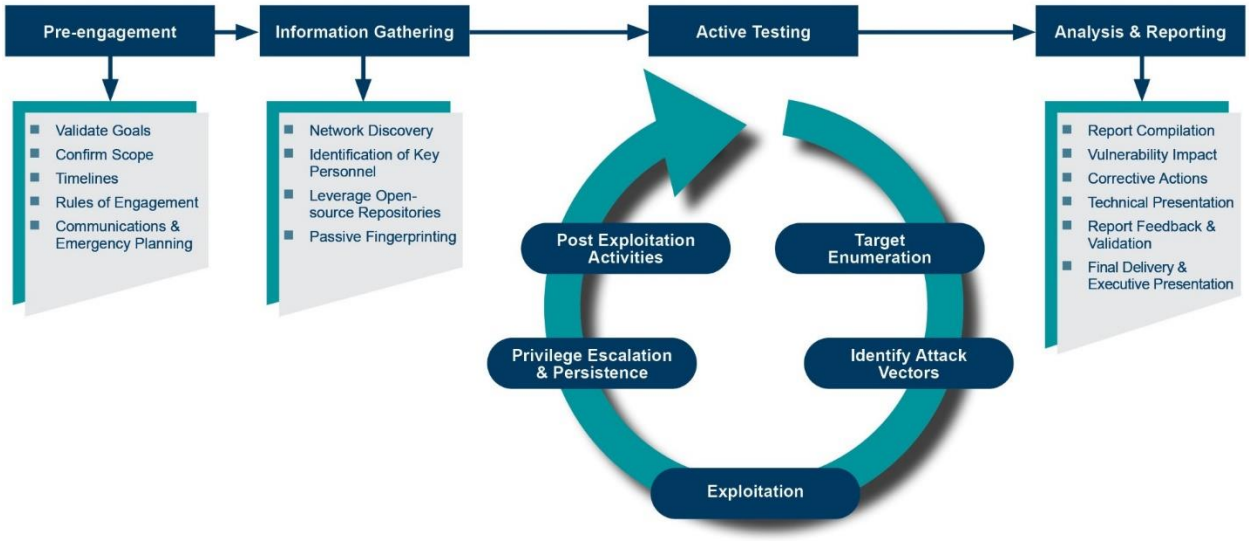
Scope Details	• Network Penetration Testing
	  ○ Two (2) weeks of effort
	  ○ External Network Penetration Testing
	  ▪ Blackbox methodology against 100 IPs
	  ○ Internal Network Penetration Testing
	  ▪ Utilize Greybox methodology, with internal access facilitated by Kudelski Security-provided virtual or physical device
	  ▪ Attempt to find vulnerabilities missed by automated techniques
	  ○ Provide recommendations on remediating findings and improving threat detection and response.
	• Retesting
	  ○ Validate the remediation of all *critical* and *high-severity* findings within 90 days of draft Findings Report delivery

Testing Window	Normal Business Hours
Scope Exclusions	• Authenticated application testing • Remediation • Onsite Testing
Deliverables	• Findings and Recommendations Report • Retest Report
Location of Services	Remote

ENGAGEMENT METHODOLOGY

Kudelski Security provides a comprehensive portfolio of offensive security services. Leveraging automated and manual processes, we identify not only complex vulnerabilities within your environment but also perform manual research and exploitation, using a sequencing approach that validates viable attack vectors in line with agreed-upon rules of engagement. We use the Common Vulnerability Scoring System (CVSS) to classify our findings and combine them with business-relevant information, such as organizational impact and attack complexity. The outcome is a remediation strategy with actions prioritized according to criticality.

The Kudelski Security team holds globally recognized industry certifications and brings to bear years of real-world experience. Our testing processes utilize the well-established Open-Source Security Testing Methodology Manual (OSSTMM) and the Open Web Application Security Project (OWASP) methodologies, as well as the principles defined in the OWASP Testing Guide, to structure their service delivery. This process ensures that only validated and confirmed results are reported. Such certifications and methodologies also enable comparison of expertise level and results – even when delivered by organizations other than Kudelski Security. This approach gives our clients a coherent view of their security testing results even when coming from different service providers.



Over the course of the engagement, Kudelski Security will provide continuous feedback, including key discovered elements and early or emergency solutions and recommendations. This way, remediation can start even before the delivery of the final report. This advantageous reporting process increases the efficiency and relevance of the tests according to the daily findings.

With regards to the final deliverable, it will include both an executive summary and a consolidated recommendations report. Each section includes actionable recommendations, a high-level summary describing the major vulnerabilities sorted by criticality, how they have been discovered and how they could be exploited by a malicious attacker to gather sensitive information. Through the systematic use of the OSSTMM and OWASP methodologies, our team follows a comprehensive framework and delivers comprehensive technical reports, which allows for comparing tests results with other pen testers applying these same standards.

PHASES AND ACTIVITIES

Phase 1: Engagement Preparation

Kudelski Security will host and lead a kick-off call with Client's sponsor and point of contact (hereafter referred to as the "designated engagement manager" or "DEM") to gather detailed information necessary to ensure a successful engagement.

The primary goals of this kick-off call are to:

- Validate that goals and scope are accurately captured in the SOW.
- Ensure activities and prerequisites are understood & coordinated prior to commencement.
- Identify any obstacles or challenges to completion that may be unique to Client.
- Identify key stakeholders from both Kudelski Security and Client who need to be included in the engagement updates and escalations.
- Agree on a secure communication path.
- Discuss and agree upon the escalation processes for critical vulnerabilities, including who should be notified, the method of notifications and what level of criticality warrants immediate notification.
- Discuss timelines for the engagement's commencement and duration.
- Agree on the process to delete any data on Kudelski Security's physical devices used for any applicable internal testing, including allowing Client to purchase the physical device(s) for the amount of $600.00 per device.

Phase 2: Data Collection

- **Information gathering** – Gathering target-specific data using open-source intelligence repositories, search engines and social media.
- **Network scan** – Scanning of the IPs to identify responsive hosts and exposed services.
- **Vulnerability scans** – In-depth interrogation of services to determine system and version information. This is essential in identifying vulnerabilities and possible attack vectors.

Phase 3: Active Testing

External Penetration Testing

- Testing will be focused against in-scope, internet-facing IP addresses.
- **Planning & Preparation** – Kudelski Security will utilize the outputs of the Data Collection phase to select techniques to bypass security controls and exploit vulnerable services. Additional vulnerability and exploitation research is conducted as necessary.
- **Exploitation** – Using techniques authorized within the rules of the engagement Kudelski Security will exploit vulnerable services and systems in order to achieve the engagement objectives.
- **Follow On Activities** – Constrained to authorized activities such as stop & report, lateral movement, password dumping, privilege escalation, and establishing persistence.

Internal Penetration Testing

- Penetration testing of IP addresses within the internal network.
- Internal access will be enabled by successful exploitation of external infrastructure or through the deployment of a Kudelski Security provided physical device or virtual appliance.
- Manual research and analysis to remove false positives and validate potential attack vectors.
- The exploitation of internally facing vulnerabilities by an advanced insider threat.
- Post-exploitation activities will be limited to those approved by the Client DEM during the engagement kick-off call and documented within the ROE. Examples of typical activities: uncover sensitive information, identify exfiltration methods, lateral movement, etc.

Phase 4: Deliverable Preparation

Kudelski Security will analyze the gathered data, develop the recommendations, and provide remediation priority. The Client DEM will need to be available in case our security engineers have any outstanding questions while they are developing recommendations. Deliverables are outlined in the section below.

Phase 5: Report Presentation

Kudelski Security will deliver a remote technical findings presentation to an audience of Client's choosing. This presentation will describe the tasks conducted and provide an overview of the engagement results.

Phase 6: Retesting

Kudelski Security will perform retesting of in-scope findings within ninety (90) days following delivery of the draft Findings and Recommendations Report. The results of this retest will be provided within the agreed-upon Deliverable format outlined below.

DELIVERABLES

NOTE: Deliverable(s) will be provided in electronic format.

Deliverable	Description
Findings and Recommendations Report	A technical report designed for Managers and Program Owners. The report will include summaries of tests performed, the observed results, the recommended mitigation techniques, and prioritization of each recommendation, based on the Client's business and risks.
Retest Report	Summarizes findings of the follow-up test to validate remediation of the findings within the scope for retesting.

Deliverable Acceptance

All material Deliverables defined in this SOW are subject to inspection and acceptance by the Client DEM. Client will agree upon and document any specific acceptance criteria with Kudelski Security during the Kickoff Call, prior to commencement of the associated work. Any special requests (such as additional content or non-standard templates) not stated within this SOW will require a Change Order.

Kudelski Security will provide for one (1) round of draft review, during which the Client will be given an opportunity to review and comment to ensure a Deliverable is complete and accurate and that it meets expectations. Client is responsible for distributing any Deliverables to appropriate stakeholders, obtaining feedback, and consolidating that feedback into a single view for Kudelski Security consultants to update appropriately. Kudelski Security will provide the finalized Deliverable for Client acceptance or rejection. If the Deliverable does not conform to the agreed-upon acceptance requirements, Client shall notify Kudelski Security in writing, setting forth Client rejection and the basis of the nonconformity. Kudelski Security shall correct such nonconformity within a mutually agreeable timeframe.

Client will accept or reject the Deliverable(s) within ten (10) business days of completing each iteration. If Client does not accept or reject the Deliverable(s) within this period, the Deliverable(s) shall be considered accepted.

PROJECT MANAGEMENT

Kudelski Security will assign a dedicated Project Manager to oversee the engagement from initiation to closure. This Project Manager is responsible for ensuring the engagement runs smoothly and expectations are met. Kudelski Security's Project Management process is broken down into three (3) high-level activities: project initiation, project execution, and project closure, as described in the table below.

Project Initiation	• Schedule and conduct engagement kick-off meeting. • Review project scope with the team and gain agreement from all parties. • Establish communication plan and templates. • Develop timeline and milestones based on input from the team. • Define team members and schedule resources based on timeline and milestones. • Define metrics for a successful engagement.
Project Execution	• Provide status updates to Client as agreed upon during project initiation. • Monitor project schedule and budget. • Deliver on the project as outlined during project initiation.
Project Closure	• Deliver all final documents as agreed upon per the proposal. • Conduct Client feedback session to identify highlights of the project and opportunities for improvement on a go-forward basis. • Coordinate invoicing between Client and Kudelski Security accounting .

Maintaining clear channels of communication will be necessary to ensure any project success. Kudelski Security will conduct status meetings, which may include updates on project status and issues identified and addressed (such as schedule, Deliverables, project quality, and team interaction). In addition, Kudelski Security will provide notification of issues requiring Client involvement. Kudelski Security expects that any issues identified will be resolved promptly to avoid impacting the project timelines.

SCHEDULING / DURATION

Kudelski Security cannot schedule services or determine engagement timelines until the SOW is mutually executed. Following SOW execution, Kudelski Security's Project Management Office ("PMO") will contact the Client to schedule a project kickoff call. During kickoff, an **Engagement Start Date** will be determined based on then-current scheduling factors for both Parties.

This SOW will expire 60 days from the Engagement Start Date unless otherwise mutually agreed upon by both Parties. Once the SOW has expired, any unpaid services or applicable expenses will be invoiced. No refunds will be provided for any prepaid services that are not scheduled and completed before SOW expiration.

Kudelski Security requires one (1) week's written notice in advance of the Engagement Start Date for cancelling or rescheduling any services. If cancellation or rescheduling occurs with less than one (1) week notice of the Engagement Start Date, Client agrees to pay a fee of $2,500 per resource assigned. Any nonrefundable and/or nontransferable travel expenses will be billed to and paid by Client at actual cost. Notices can be sent to: KSIPMO@kudelskisecurity.com.

ACKNOWLEDGMENTS

Client acknowledges that the performance of the services herein may involve the use of techniques and tools, including (but not limited to) security vulnerability scanning, penetration testing, static analysis, and manual code review of computer systems, applications, and IT infrastructure. Client duly authorizes Kudelski Security and its agents to conduct security verification activities by using such techniques and tools.

Client represents warrants and covenants that it has—and will maintain—the authority to appoint Kudelski Security and that it has the legal right to subject the assets, systems, applications, and infrastructures that are part of the engagement ("the assets") to the Services and that if it is not the owner of the assets, it has obtained such right from the owner of such assets. Client acknowledges and agrees that Kudelski Security shall not be liable for any and all damages claimed by the owner or right holder of the assets subject to the Services and Client shall indemnify and hold harmless Kudelski Security from any and all damages arising from such claims.

Client further acknowledges and agrees that:

- It has the sole responsibility for the adequate protection data and assets used in connection with and/or impacted by the Services. Client will, among other measures, set up a backup and recovery procedure enabling the restoration of data, assets and services to their pre-assessment state.
- In rare circumstances, services may slow or otherwise impact the assets operations. Kudelski Security adheres to industry best practices to avoid unexpected impacts.
- Services' results relate to specifically designated techniques and tests and are not meant to provide Client with a comprehensive assessment of all security and configuration issues.

- The performance of the Services necessarily requires the use of network tools and techniques designed to identify security vulnerabilities, and that it is impossible to identify and eliminate in advance all the risks and consequences involved in the use of these tools and techniques.
- The inherent nature of penetration testing cannot guarantee the exposure or detection of all weaknesses or vulnerabilities. Consequently, Kudelski Security provides no warranty or guarantee as to the outcome of the testing or assessment methods and Client knowingly accepts these limitations and risks. This disclaimer is in addition to and not a substitute for any other disclaimers and limitation of liability in this document.

ASSUMPTIONS

- Kudelski Security resources will perform all work remotely unless otherwise mutually agreed to.
- Kudelski Security resources will have adequate access to Client employees involved in this engagement, both technical and business, to complete activities in a timely fashion.
- Kudelski Security resources will have appropriate access to information, systems and/or networks necessary in performing the engagement.
- Delays in receiving necessary information may impact the engagement schedule.
- Kudelski Security resources are limited to no more than 15 consecutive hours of work. If additional hours are required, the Project Manager may utilize additional resources (with approval).
- Kudelski Security resources will not work on a recognized holiday unless mutually agreed to in writing. A list of recognized holidays will be provided by Kudelski Security upon request.

CHANGE CONTROL

Kudelski Security will not perform any additional work outside of the scope described in this SOW without a signed Change Order. If unforeseen factors affect the scope or effort of the project, Kudelski Security will provide a Change Order for Client to review and sign before any work outside the original scope is performed or additional expenses are invoiced to Client. The Change Order will specifically address any variance from the original SOW and the associated costs and provide a brief explanation of the requirements for the changes.

COMPLETION AND ACCEPTANCE

Upon completion of the services, (or applicable portion), including any Deliverables, Kudelski Security will provide written notification to the Client DEM indicating completion and requesting written acceptance / acknowledgement. Client will promptly review the notification and provide a written response. If this response indicates that Kudelski Security has not satisfactorily completed the services, the parties will discuss or meet and use good faith to resolve the issues. If Client does not respond in writing within ten (10) business days of receipt of Kudelski Security's notice of completion, then the services are considered accepted.

ENGAGEMENT RESPONSIBILITIES

Responsibilities of Kudelski Security

- Directly manage Kudelski Security resources, excluding any Client-contracted consultants or third parties, unless agreed to in writing.
- Follow all reasonably written security rules and procedures provided by Client.
- Serve as the primary point of contact for the life of the engagement.
- Facilitate the engagement kick-off meeting.
- Manage the engagement budget and Change Order process (if needed).
- Coordinate Kudelski Security personnel logistics.
- Prepare and deliver status reports on regular intervals as mutually agreed to.
- Ensure engagement work is completed as agreed upon in the SOW and obtain sign-off.

Responsibilities of Client

- Provide an employee to serve as the DEM. The DEM will be responsible for scheduling Client resources for required meetings, interviews, and other needs deemed necessary to complete the project work as scoped. The DEM will serve as the first point of escalation for any project-related requests or issues.
- For any assets that are not hosted or do not belong to the Client, attain written consent from the third party to perform a penetration test on those assets prior to the Engagement Start Date.
- Provide access with necessary consents, permissions, and authorizations to all proprietary information, hardware and software applications, and other systems necessary, whether owned, leased, or licensed, before starting services and until services are completed.
- Execute all data gathering activities in an efficient manner and submit data to Kudelski Security consultants within a commercially reasonable response time. Any delays incurred in acquiring this information may result in the need for a Change Order and rescheduling of the engagement, at the discretion of Kudelski Security.
- Provide the necessary staff availability to complete identified tasks and/or to participate in interviews to ensure the agreed upon completion dates, tasks, or Deliverables.
- Provide access to any necessary facility and/or remote access to complete the engagement during normal business hours or other agreed times.
- Perform a complete back-up of all data and software prior to the start of services.
- Client agrees to Kudelski Security's use of Client as a reference on a case-by-case basis with future Kudelski Security prospective clients. Kudelski Security and Client agree that references will remain private between Kudelski Security, Client, and the prospective client(s) and will not be made public, including but not limited to social media or Kudelski Security's printed marketing materials without the written consent of Client.

CONTACT INFORMATION

NAME	FUNCTION	PHONE	EMAIL
CLIENT CONTACTS			
Ben Sanders	Security Director	409-797-3748	basanders@galvestontx.gov
KUDELSKI SECURITY CONTACTS			
Matt Davis	Regional Sales Manager	512-401-8623	matt.davis@kudelskisecurity.com
Troy Dearing	Director, Offensive Security Services	480-438-1923	troy.dearing@kudelskisecurity.com
Michael Moretina	Director, Project Management Office	602-451-7337	michael.moretina@kudelskisecurity.com

PRICING

Kudelski Security will bill this project on a Firm Fixed Fee ("FFF") basis. All amounts shown in USD currency and exclusive of applicable taxes.

Service	FFF
Network Penetration Testing	$22,500

Invoicing and Payment

- Kudelski Security will invoice Client for 50% of the FFF upon execution of the SOW and 50% upon submission of draft Deliverable(s).
- Payment terms for all invoices are NET 30 days from invoice date.

EXECUTION OF SOW

By the signatures of their duly authorized representatives below, the Parties, intending to be legally bound, acknowledge, understand, and agree to all provisions of this SOW. If this SOW is not signed within 30 days of the publish date, all services, terms, and prices herein may be subject to change and/or rescoping.

Kudelski Security, Inc.	**City of Galveston, Texas**
Authorized Signature	Authorized Signature
Name (Print)	Name (Print)
Title	Title
Date	Date