TrustedSec

Version 1.0 | April 25, 2022

2022 Incident Response Retainer Proposal

Prepared for:

City of Lexington

200 East Main St.

Lexington, KY 40507

April 25, 2022

Prepared for:
City of Lexington
200 East Main St.
Lexington, KY 40507

Contained within this Statement of Work (SOW) are the methodologies around incident response services.

TrustedSec's Incident Response team will investigate security incidents that may affect the confidentiality, availability and integrity of data by assisting in containing, eradicating, and guiding the response to remediate the situation.

TrustedSec's IR team delivers on three main tenets for our clients:
Faster Resolution – TrustedSec is a global leader in attack intelligence, bringing to bear the latest hacker tactics and techniques to quickly get to the bottom of an incident.
Personalized Attention –TrustedSec remains engaged throughout the entire process and facilitates collaboration holistically to address any unique challenges the organization may face.
Defensibility –TrustedSec works with clients to put them in the best defensible position possible, creating a meaningful action plan to address any issues discovered.

We appreciate the opportunity to present this proposal to City of Lexington and look forward to a long-lasting partnership. If there are any questions, please feel free to contact us at any time.

David Thompson | Account Manager
TrustedSec
14780 Pearl Road, Suite 300
Strongsville, OH 44136
Office: 877.550.4728 x7013
Mobile: 440.864.3874
Email: David.Thompson@TrustedSec.com

Document Disclaimer Statement

This disclaimer governs the use of this document. Client shall own all right, title, and interest in and to any written summaries, reports, analyses, and findings or other information or documentation prepared for Client in connection with TrustedSec, LLC, its agents, officers, directors, employees, affiliates, and assigns (collectively 'TrustedSec') consulting services to Client. TrustedSec expressly disclaims any and all liability for any damages whatsoever (whether foreseen or unforeseen, direct, indirect, consequential, incidental, special, exemplary, or punitive) arising from or related to reliance by anyone on this document or any contents thereof.

Copyrights and Trademarks

TrustedSec Confidential

This document has been classified as TrustedSec Confidential. This is an internal TrustedSec designation, which has the highest classification ranking for Client data. Stringent protection of this document is required by TrustedSec's information classification policy and security controls. Additionally, the information contained in this document is strictly prohibited from any type of release except to the Client.

Addendum

As this role would expose personal information on LFUCG's systems to TrustedSec, I'd suggest the following language be added, pursuant to KRS 61.932:

TrustedSec agrees that its security and breach investigation procedures of personal information (as defined in KRS 61.931) in its possession from LFUCG complies with KRS 61.392(2)(a). TrustedSec further agrees to comply with the notice requirements contained in KRS 61.392(2)(b) for security breaches (as defined in KRS 61.391) on its systems related to the personal information obtained from LFUCG pursuant to this Agreement. The cost of notification and investigation requirements under KRS 61.933 for security breaches on TrustedSec systems related to the personal information obtained from LFUCG pursuant to this Agreement shall be paid entirely by TrustedSec. This paragraph shall survive the termination of this Agreement.

Table of Contents

1 Engagement Process

1.1 Engagement Coordination

TrustedSec believes strong, open, and continual communication is vital to the success of all engagements. Engagement Coordinators work with clients to best align the consulting team's expertise with the engagement's scope and timeline. Every engagement begins with a series of dialogues to identify the goals and objectives of the assessment to ensure that all expectations are exceeded. As part of the engagement team, a consulting lead will be established as the primary point of contact for executing the assessment. It is their responsibility to ensure timely communication during the engagement while monitoring established milestones.

Assigned personnel will be accessible, working closely to guarantee a collaborative and open communication strategy. Upon request, TrustedSec can also deliver assessment updates and the overall status. TrustedSec consultants will be readily available and can be reached by phone, email, or in-person if onsite. This availability also extends beyond the engagement should questions of points of clarification arise.

Should a critical or high-severity deficiency be identified, it will be communicated immediately along with remediation details. Open communication is vital during any engagement type, and TrustedSec will ensure that City of Lexington can quickly reach the appropriate points of contact.

1.2 TrustedSec File Sharing

When working with TrustedSec, City of Lexington points of contact (PoCs) will be enrolled in the TrustedSec Hub (TSHUB) Client Portal hosted onsite in the TrustedSec datacenter. This portal is used to enable file transfers, share engagement documentation, and provide an easy way to facilitate communication securely. TSHUB uses military-grade encryption for all client containers, with all client files stored in an encrypted format on disk and at rest in their own individual encrypted container. The site itself supports multi-factor authentication and ensures the highest level of security requirements for our clients.

For clients who are unable to use the TrustedSec file-sharing system, TrustedSec can use City of Lexington's file-sharing service, PGP-encrypted emails, or encrypted (AES256) zip files.

2 Incident Response/Forensics

TrustedSec's Incident Response team is focused on helping clients recover from Information Security events while minimizing the impact of the event on the organization. Whether the incident is caused by a malicious insider or an external attacker, or a large-scale breach has taken place, TrustedSec can provide Incident Response and Forensic Analysis services.

TrustedSec consultants draw on a range of unique skills, experience, and technology to investigate each incident, contain the situation, eradicate the attacker, and remediate the environment. TrustedSec utilizes industry-standard, top-class hardware and software while performing Incident Response and Forensic Analysis activities to ensure quick and accurate results. The techniques used by TrustedSec are admissible in a court of law and ensure appropriate chain of custody and the highest standards of quality.

The major activities TrustedSec performs during an investigation consist of the following:

2.1 Assess

Each investigation begins by gaining an understanding of the current situation. Approximately when did the incident take place? How was the issue detected? What individuals, departments, business units, and physical locations have been impacted? What forensic data has been collected? What steps have been taken? What does the environment look like? Who are the main points of contact for incident communication?

2.2 Client Objectives

The next step is to define objectives that are practical and achievable. The goals may be to identify if there has been any data loss, strictly recover from the incident, identify the attack vector used, attribute the attack to a specific actor, or a combination of these examples.

2.3 Investigate

TrustedSec Incident Response consultants collect information using forensically sound procedures and document evidence-handling with chain of custody procedures that are consistent with law enforcement standards.

When investigating physical disks, TrustedSec utilizes industrial-grade write blockers, forensics equipment, and forensically sound analysis tools. TrustedSec will ensure the following:

- Evidence is admissible in litigation scenarios
- Proper handling of evidence with rapid discovery and acquisition
- Clear and concise results around what was discovered

Should it be necessary, TrustedSec can deploy software and hardware across the environment to gain visibility into endpoints and networks, search for Indicators of Compromise, obtain data in a forensically sound manner, and monitor for malicious activity.

2.4 Analyze

Based on the evidence that is available and the client's objectives, TrustedSec may analyze data to determine the attack vector used, establish a timeline of incident activity, and identify the extent of the compromise including, but not limited to, the following sources:

- Forensic, system, or log data obtained from systems of interest;
- Network-related activity, packets, or logs;
- Attacker tools, malware, or malicious documents;
- Documentation of client systems, networks, and architectures; and
- Logs obtained from systems, network devices, or centralized logging infrastructures.

TrustedSec analysts are highly trained with professional experience in the private and government sectors, and only private, top-level senior resources are used when performing any type of forensic analysis. TrustedSec's experts are here to assist in any situation and respond to incidents as they happen.

2.5 Provide Direction

During each investigation, TrustedSec works closely with the client management team to establish a predetermined communication and reporting cadence. Detailed status reports will provide up to date incident tracking, communicate critical findings, and equip clients with the tools necessary to make the correct business decisions.

2.6 Containment, Eradication and Remediation Plan

Remediation plans vary depending on the extent of the compromise, the size of the organization, the capabilities of the client infrastructure, and the tactics/objectives of the attacker. As part of an investigation, TrustedSec delivers a comprehensive containment, eradication, and remediation action plan. Assistance with plan implementations can be performed utilizing TrustedSec's Remediation Services team.

2.7 Reporting

TrustedSec provides a detailed investigative report at the end of every engagement that addresses the needs of multiple audiences, including senior management, technical staff, third-party regulators, insurers, and litigators.

The investigative reports contain sections such as an executive summary, incident event timeline, critical incident findings, associated threat intelligence, and malware analysis.

2.8 Remote Incident Response

TrustedSec has created custom devices that allow TrustedSec to perform remote Incident Response services for clients. TrustedSec has the ability to quickly deploy these remote devices, which can be connected at any point of the network, establishing a secure tunnel back to the TrustedSec headquarters. This device allows TrustedSec to perform Incident Response services without requiring consultants to be on-site and allow the monitoring of client networks. This helps to not only reduce travel expenses but decreases the burden on consultant travel and allows additional consultants to join and collaborate on the assessment.

These systems were developed internally by TrustedSec and have been improved proactively over the years. The devices are preconfigured with all the tools that consultants are accustomed to using during an assessment. This option is highly recommended for remote locations, long-term contracts, and more.

Note: These devices must be returned to TrustedSec within four (4) weeks of report delivery. Failure to do so will result in a fee of $2,500.

Additionally, TrustedSec may wish to deploy and utilize commercial endpoint software to gain visibility into client endpoints. TrustedSec will work directly with the client to determine if this is possible, the best method for deployment, and any configuration changes that may be needed for the software to communicate back to TrustedSec centrally secured servers. If used, additional tools fees may be applied.

3 Statement of Work

This **STATEMENT OF WORK** ("SOW"), effective as of April 25, 2022 is made pursuant to an agreement by and between **TrustedSec, LLC** with its principal place of business located at 14780 Pearl Road, Suite 300, Strongsville, Ohio 44136, and **City of Lexington**, with its principal place of business located at 200 East Main St. Lexington, KY 40507.

3.1 Engagement Scope

This section contains the overall scope for the engagement, as discussed with City of Lexington. Based on TrustedSec's understanding of the environment, we have scoped the time and cost of the proposed services with the assumptions below. If it is determined that there is a vast difference in the actual environment (either smaller or larger), TrustedSec requests the right to adjust the actual effort required and costs associated with the assessment. Any cost estimate or timeline changes needed will be promptly shared with City of Lexington, and a Change Order will be drawn as appropriate to satisfy the changes. This is uncommon; however, it can happen based on additional discoveries or further evaluation from TrustedSec.

Geographic Locations

- TrustedSec Headquarters, Cleveland, OH, US

TrustedSec Incident Responders are flexible in their hours and will work with the client as needed.

Incident Response Retainer

- 40 hours of Incident Response Retainer Services and Reporting
- Priority scheduling in the event of an incident
    - Initial contact with client using email or phone within four (4) hours of notification to TrustedSec through approved channels
    - Approved channels to notify TrustedSec in the event of an incident are:
        - Email *IR@TrustedSec.com*
        - Call 1-800-246-2792, option 1
    - Remote work is to begin within 24 hours of contact with client, if there is an existing retainer
    - Additional hours may be purchased in 40-hour increments.
    - Hours are valid for 12 months from contract execution date
        - Unused hours may be utilized toward additional TrustedSec services, excluding any incident response services (tabletop/playbook exercises and or threat hunt exercises), red/blue/purple team exercises, and or IoT/Hardware assessments

- Retainer hours and Service Level Agreements (SLAs) activate 10 business days from date of contract execution
- Incident evidence will be stored by TrustedSec for six (6) months after the draft report is delivered
- Any physical, verbal, or emotional abuse directed at TrustedSec consultants including, but not limited to, harassment and abusive language will not be tolerated. Any abuse or harassment by City of Lexington representatives, employees, affiliates, or partners, directed at TrustedSec consultants will allow immediate termination of the contract and the client shall pay for all work performed with a minimum of 25% of total quote. TrustedSec shall transfer all working documents to the client and shall not be responsible for any further deliverables.

Out of Scope:

- Any location or work that is not specifically listed as in-scope shall be considered out of scope

Dependencies and Assumptions

The following terms are set forth to determine the roles and responsibilities that both parties are to maintain. This is done to eliminate confusion and prevent delays in onsite data gathering. Failure to maintain these terms may result in extended data collection, additional labor fees, and related travel expenses to cover the extra time spent.

- Scoped pricing is based upon the information provided by City of Lexington via initial discovery documents/conversations with TrustedSec prior to the start of the engagement. Additional applications, divisions, domains, or systems found during the discovery phase of the engagement that are not stated in the scope of work will incur additional fees, and may result in the need for an agreed upon Change Request.
- The work is to be performed consecutively until engagement completion. There will be no break in services other than weekends and/or recognized holidays.
- TrustedSec assumes that all client data gathering activities will be executed efficiently, and data will be promptly submitted to consultants. Any delays incurred in acquiring this information may result in the need for a mutually agreed upon Change Request.
- Client will designate one (1) employee to serve as a primary point-of-contact (PoC) for the TrustedSec engagement team. The client-designated PoC will be responsible for and have the authority to schedule client resources for required meetings, interviews, and other needs to complete the work within the specified engagement parameters.
- Where applicable, Client is responsible for notifying impacted third parties of the testing as needed, and said testing is conducted with the expressed authority of Client Officers or Directors (See Notice in Document Disclaimer Statement).
- No TrustedSec employee is expected to work more than ten (10) consecutive hours.

- Client will provide access to all proprietary information, applications, and systems necessary to the success of this engagement.
- Any special conditions not stipulated at the time of this quotation, such as late evening/early morning hour requirements, may result in additional fees.
- TrustedSec will not perform any additional work outside of the scope of work described in this proposal without the expressed permission of authorized personnel of City of Lexington, including a signed Change Order.
- Assessments (excluding Incident Response) will be performed during normal business hours 8:00 AM - 5:00 PM. Should assessments be performed during off-hours, an additional cost will be sent through a change order.

Rescheduling Fee

Aligning resources to provide the most value to our clients is a constant challenge. TrustedSec will always make every effort to meet any needs of City of Lexington. However, if there are any changes to the schedule required by City of Lexington once a start date for the services being provided under this SOW has been agreed upon, a rescheduling fee may be charged as per the following schedule:

- Greater than 10 business days: No rescheduling fee will be charged.
- Less than 10 business days but greater than five (5) business days: A 10% rescheduling may be charged.
- Less than five (5) business days: A 50% rescheduling fee may be charged, in addition to any fees incurred (such as airline tickets, etc.) if applicable.

3.1.1 Incident Response Deliverables

Executive Summary

- An Executive Summary will be produced at the conclusion of the assessment, summarizing the objectives of the engagement, work performed, findings and remediation strategy. The Executive Summary is, by default, a part of the technical report, unless otherwise indicated during the scoping process.

Technical Report

- The document details the Technical Findings and Strategic Recommendations regarding any identified weaknesses in the environment. The document will also articulate the work performed, list the steps to reproduce each issue, and provide Severity Ratings for each vulnerability. The initial draft report will be targeted for delivery as a PDF within two (2) weeks of the conclusion of the overall engagement effort. If requested, one (1) round of revisions to the report may be provided within three (3) months of delivery of the initial report.

Presentation of Findings (Upon Request)

- If requested, the TrustedSec findings presentation will be delivered remotely via web conference to the audience chosen by City of Lexington. Traditionally focused on an executive-level out-brief, this presentation describes the effort executed, provides an overview of the results, and describes the next steps outlined for the organization.

4 Engagement Pricing

The fixed fees for the Services to be performed by TrustedSec under this SOW are in US dollars and are detailed in the table below. Acceptance of this SOW authorizes TrustedSec to perform a security assessment and other related services for City of Lexington. Proposal is valid for 30 calendar days.

Service	Description	SKU	Cost
Incident Response Retainer	40-hour retainer for Incident Response Services.	TS-54000	$16,000
Tools Fees	Fees for usage and storage of endpoint visibility software.	TS-54600	Billed at actuals
		Total Engagement Cost	**$16,000**

4.1 Payment Schedule

Payment is based on the following schedule:

- 100% of total cost due at contract execution. Payment terms Net 30.
- A 5% late fee will be added for payments that exceed payment terms.
- Report delivery is subject to the terms and conditions set forth within this statement of work.
- Acceptable forms of payment are check, ACH, or wire transfer.

4.2 Travel & Expenses

TrustedSec fees outlined in the scope of services do not include out-of-pocket expenses, such as transportation, meals, and lodging for travel to perform any of the services. TrustedSec will make every attempt to incur reasonable expenses associated with the execution of the engagement and will handle the processing of those approved expenses in accordance with the Travel Policy terms from the Master Services Agreement. Valid expenses typically include parking, meals, lodging, and communication costs. Travel costs include airfare, mileage (if a personal car is used), and automobile rental. If international travel is required, additional expenses may be incurred, including business class ticketing on flights. TrustedSec consultants use business class when the combined flight connection exceeds 3,400 miles in a single direction.

4.3 Change in Scope of Services

If unforeseen factors change this scope of work and/or impact the term and cost of provided services, City of Lexington and TrustedSec may mutually revise the SOW. TrustedSec shall provide City of Lexington with an estimate of the impact of such revisions on the fees, payment terms, completion schedule, and other applicable provisions of the SOW. If the parties mutually agree to such changes, a written description of the agreed change (Change Order) shall be prepared, incorporating such changes to the SOW and shall be signed by both parties. The terms of a Change Order Form prevail over those of the SOW.

4.4 Authorization

By the signatures of their duly authorized representatives below, City of Lexington and TrustedSec, intending to be legally bound, agree to all the provisions of this Statement of Work as of the Effective Date set forth below.

Printed Name for City of Lexington	Printed Name for TrustedSec, LLC
Title [Must be Officer or Director]	Title
City of Lexington Signature	TrustedSec, LLC Signature
Date	Date