2021 Blue Team Guidance Proposal
Version 1.0

March 2, 2021

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

March 2, 2021

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

Contained within this Statement of Work (SOW) are the methodologies around blue team guidance services.

TrustedSec's Defense engagements are designed to evaluate the effectiveness of the operational security program, with a focus on Detection, Deflection, and Deterrence. The engagement is designed to provide more value to City of Lexington's defenses with tangible improvements in the ability to address attacker behavior. TrustedSec's team will provide direction for implementing changes, and strategies for better visibility, understanding of activity and increased alignment between teams.

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 x713
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 specifically 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 any guidance in 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. This document should never be communicated from TrustedSec to the Client in an unencrypted format. Additionally, the information contained in this document is strictly prohibited from any type of release except to the Client.

Table of Contents

1 ENGAGEMENT PROCESS 5
1.1 ENGAGEMENT COORDINATION 5
1.2 TRUSTEDSEC FILE SHARING 5
1.3 REPORT TIMING 5
2 DEFENSIVE COUNTERMEASURE GUIDANCE (BLUE TEAM GUIDANCE) 7
2.1 PENETRATION TEST RESULTS REVIEW 7
2.2 SECURITY POSTURE EVALUATION 7
2.3 BLUE TEAM GUIDANCE 7
3 STATEMENT OF WORK 8
3.1 ENGAGEMENT SCOPE 8
3.1.1 TECHNICAL DELIVERABLES 10
4 ENGAGEMENT PRICING 11
4.1 PAYMENT SCHEDULE 11
4.2 TRAVEL & EXPENSES 11
4.3 CHANGE IN SCOPE OF SERVICES 12
4.4 AUTHORIZATION 12

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, in order 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 the execution of the assessment. It is their responsibility to ensure timely communication during the engagement, while monitoring established milestones.

Assigned personnel will always be accessible, working closely to guarantee a collaborative and open communication strategy. Upon request, TrustedSec can also deliver status updates on the assessment and the overall progress. The status updates will include levels of effort, progress for the assessment, and any new information since the prior status update. TrustedSec consultants will be readily available during the assessment and can be reached by phone, email, or in person while on-site. This availability also extends beyond the engagement, should questions of points of clarification arise during City of Lexington's review and remediation process.

During the engagement, should a critical or high-severity deficiency be identified, it will be communicated immediately, along with remediation details, prior to the delivery of the report. Open communication is important during any engagement type and TrustedSec will ensure that City of Lexington can reach the appropriate points of contact at any time.

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 on-site in the TrustedSec datacenter. This portal is used to facilitate file transfers, share engagement documentation, and provide an easy way to securely facilitate communication. 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 own file sharing service, PGP-encrypted emails, or encrypted (AES256) zip files.

1.3 Report Timing

Unless otherwise defined under this Statement of Work (SOW), within two (2) weeks of conclusion of the work described above, TrustedSec will issue a formal draft report to the

primary PoC. TrustedSec shall make every reasonable effort to promptly correct any inconsistencies identified by City of Lexington and shall resubmit the deliverable for City of Lexington's review. If there are no comments within the two-week comment period, TrustedSec will consider the report final.

2 Defensive Guidance (Blue Team Guidance)

2.1 Penetration Test Results Review

Blue Team Guidance engagements are conducted remotely for the target organization and use the organization's previous penetration test report as a reference point to provide defensive insight and recommendations.

2.2 Security Posture Evaluation

TrustedSec believes an organization's security posture is best evaluated by identifying the defensive controls around these three (3) abilities:

Detection – The ability to detect an attack through multiple phases of a compromise. This is foundational to reducing any potential damage inflicted during a breach.

Deflection – Focuses on placing attackers in environments or situations to increase the difficulty in attacking or planting deception in the network. This focuses the attack in other areas that may have higher detection capabilities.

Deterrence – Also referred to as protection—the ability to build proactive measures that directly defend the network through protection. Where protection cannot be implemented, enhancements to Detection and Deflection are necessary.

2.3 Blue Team Guidance

Consultants analyze the penetration test results against these abilities, evaluate SIEM ingestion and effectiveness, security operational procedures, and provide guidance for improvement in detection, defelection, and deterrence abilities.

3 Statement of Work

This **STATEMENT OF WORK** ("SOW"), effective as of March 2, 2021 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 required will be shared with City of Lexington promptly, 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

Blue Team Guidance

- Work will be performed by one (1) remote consultant
- Previous penetration test report analysis and attack customization
- SIEM rule analysis
- Analysis of deflection and deterrence controls

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 on-site data gathering. Failure to maintain these terms may result in extended on-site data collection, additional labor fees, and related travel expenses to cover the extra time spent on-site.

- 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 and/or systems found during the discovery phase of the engagement that are not stated in scope of work will incur additional scoping, services, or fees, and may result in the need for a mutually 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 in an efficient manner and data will be promptly submitted to TrustedSec 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 authority to, the scheduling of client resources for required meetings, interviews, and other needs deemed necessary 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 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 5 business days: A 10% rescheduling may be charged.
- Less than 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 Technical 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

- A document detailing 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.

Attestation Letter (Upon Request)

- If requested, a City of Lexington-facing document summarizing the effort and methodology that was executed and provides assurance that City of Lexington actively performs their due diligence with regard to third-party validation of Information Security controls (relative to those phases included in the given assessment engagement).

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
Blue Team Guidance	Analysis of previous penetration test results and providing appropriate guidance on SIEM adjustments to improve the defensive security posture.	TS-53400	$12,000
		Total Engagement Cost	**$12,000**

4.1 Payment Schedule

Payment is based on the following schedule:

- 50% of total cost due at contract execution. Payment terms Net 30.
- 50% of total cost due after the draft report is delivered. 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 and 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