Request for Proposal (RFP)

for

Cybersecurity Assessment

TPL Insurance

1. Introduction

TPL Insurance invites qualified and experienced cybersecurity firms to submit proposals for a cybersecurity assessment and security hardening project. The focus will be on securing three key areas pertaining to only assets and applications that are under the TPL Insurance.

1. Network and Infrastructure Vulnerability Assessment

2. Ransomware Preparedness and Risk Assessment

3. Application Security and Vulnerability Assessment

Network / Infra Assessment - Scope

1. Internet Router
2. Core Switch (1)
3. Firewall (NGFW and WAF)
4. Servers (5)
5. Exchange Server
6. Active Directory (1)
7. SIEM Solution (1)

Objective:

Evaluation of our organizations IT infrastructure, including computer systems, networks, and applications, to identify potential security risks and vulnerabilities.

Applications Assessment - Scope

1. Core Insurance Management System

2. Core Health Information System

3. TPLI Mobile App (Android / ios)

4. TPL Insurance Website

2. Objectives

The objectives of this project include:

➢ Cybersecurity Network and Infra Assessment:

1. Conduct a detailed assessment of the specified network components.
2. Identify vulnerabilities, weaknesses, and potential threats.
3. Evaluate existing security policies and procedures.
4. Perform an exhaustive examination of the network architecture, including routers, switches, servers, firewall, Exchange Server, and Active Directory.
5. Analyze the configuration and connectivity of each component to identify any potential security gaps.
6. Assess the physical and logical infrastructure to ensure a comprehensive understanding of the network's layout.
7. Identify weak points in the system, such as outdated software, misconfigurations, or unauthorized access points.
8. Evaluate the susceptibility of the network to common and emerging cyber threats.

➢ Ransomware Preparedness and Risk Assessment

1. Ransomware preparedness assessments to identify and track down any vulnerabilities that ransomware actors could exploit.

2. Ransomware assessment should enable our organization to reduce the potential damage of ransomware attacks by examining 14 crucial security areas and attack vectors to help build smarter defenses, close exploitable gaps, better safeguard sensitive data and more quickly respond and recover from an attack.

3. The assessment should focus on the cyber kill chain, including remote access configuration, phishing prevention, email and web protections, access controls, endpoint monitoring and end user awareness.

➢ Cyber Security Applications Assessment

1. To perform a comprehensive assessment, utilizing manual and automated application security testing techniques to identify and verify risks.

2. Produce an application security report that reports on anything that raises the attack surface from a runtime perspective of modern applications, back-end web services, or thick clients.
3. Since the project timeline is finite, priority should be given during testing efforts to areas of the application that, if compromised, would be of the most value for an adversary or could have the largest impact if compromised.

- **SOC Maturity Assessment**
  8. Conduct a detailed assessment of the specified SOC component it means the people, process and technology.
  9. Conduct assessment on the standard of SOC CMM.
  10. Assess SOC technology (SIEM) gaps in terms of implementation and usage.
  11. Assess SOC use cases against the MITRE framework.
  12. Assess SOC technology stack in terms of effectiveness and capability.

- **Documentation:** The documentation should be in line with SECP and ISO27001 Cyber Security Framework Compliant.
  - Provide Detailed assessment reports for each specified component.
  - Deliver a comprehensive remediation guide with actionable point for identified vulnerabilities/gaps

3. Scope of Work

The selected vendor will be required to:

13. Perform an in-depth cybersecurity assessment of the specified components.
14. Propose and implement security hardening measures specific to the identified components.
15. Collaborate with our IT and security teams throughout the project.
16. Engage in a thorough examination of the network infrastructure, meticulously analyzing the configuration, traffic patterns, and access controls of the specified components.
17. Deliver comprehensive reports detailing the findings of the cybersecurity assessment, including a prioritized list of vulnerabilities and weaknesses.
18. Present clear and actionable recommendations for addressing each identified issue, accompanied by a detailed remediation plan.
19. Document the entire assessment process, ensuring transparency and traceability in understanding the rationale behind recommendations and remediation steps.

4. Proposal Submission Guidelines

Interested vendors are requested to submit their proposals by [insert deadline].

Proposals should include:

20. Overview of the vendor's experience in cybersecurity assessments and security hardening, with a focus on similar network components.
21. Proposed methodology for conducting the assessment and implementing security hardening measures for the specified components.
22. Detailed breakdown of costs, including fees, expenses, and any additional charges.
23. References from previous clients with similar project requirements.

5. Evaluation Criteria

Proposals will be evaluated based on the following criteria:

24. Relevant experience and expertise in securing the specified network components.
25. Proposed methodology and approach tailored to the provided scope.
26. Cost and value for money.
27. References and client testimonials.

6. Timeline

The project is expected to commence 15th March 2024 and conclude by 20th April 2024 with complete documentation and deliverables.

7. Proposal Submission

Please submit your proposal by Feb 23rd 2024 to:

Name: Shaharyar Asif

Title: Team Lead Information Security

Company: TPL Insurance

Contact Number: 0301 8582325

Email Address: shaharyar.asif@tpltrakker.com

Copy/Escalations : sadaf.shaikh@tplinsurance.com

TPL Insurance reserves the right to reject any or all proposals and to negotiate with the selected vendor.

Thank you for considering our request.