**ТЕНДЕРНАЯ ДОКУМЕНТАЦИЯ**

**СОДЕРЖАНИЕ:**

1. **Инструкция для участников тендера**
2. **Приложение №1 ГОТОВАЯ ФОРМА № 1 (КОНВЕРТ №2)**
3. **ПРИЛОЖЕНИЕ №2 ГОТОВАЯ ФОРМА № 2 (КОНВЕРТ №3)**
4. **ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Инструкция для участников тендера

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Предмет тендера (закупки).**

* 1. ЗАО «Банк Компаньон» (далее Покупатель) приглашает Вас представить предложения на проводимый тендер **по выбору поставщика на поставку программного обеспечения Fortrify SAST + DAST.**

**2. Квалификация участников тендера.**

* 1. Все Участники тендера включают в состав тендерной заявки следующую информацию и документы:

1. Подтверждение об отсутствии задолженностей (налоговой и соц. фонд.)
2. Подтверждение об отсутствии судебных разбирательств за последние два года.
3. Документы, подтверждающие квалификацию согласно запросу в приложении №1 к данной инструкции.

Гарантировать предоставление нижеперечисленных документов компании, выигравшей тендер:

1. Заверенные в установленном законом порядке копии с оригинала документов, определяющих юридический статус, место регистрации и основной вид деятельности (учредительные документы, свидетельство регистрации, копия устава, копия решения полномочного органа о назначении руководителя, копия паспорта руководителя, доверенность на лицо, имеющее право деятельности);
2. Информация о наличии/отсутствии просроченной задолженности по налогам, выплатам в Социальный фонд.

**3. Затраты на участие в тендере.**

3.1. Участник непосредственно несет все затраты, связанные с подготовкой и подачей своего тендерного предложения. Покупатель ни в каких случаях не несет каких-либо обязательств или какой-либо ответственности за такие затраты.

1. **Содержание тендерных документов Участника тендера.**

Тендерные документы передаются на электронный адрес: [tender@kompanion.kg](mailto:tender@kompanion.kg) **в архивированном документе (.rar) с установленным паролем в трех электронных конвертах.**

**Внимание! Согласно правилам информационной безопасности ЗАО «Банк Компаньон» максимальный размер электронных писем не должен превышать 20МБ. В связи с этим просим Вас разделять отправляемые файлы в случае превышения данного лимита.**

**Пароль (ключ) от электронного предложения на адрес:** [pass@kompanion.kg](mailto:pass@kompanion.kg) **с указанием наименования мероприятия.**

* 1. Участник тендера должен подготовить оригинал и копии прилагаемых готовых форм тендерного предложения. Ответственность за одинаковое содержание оригинала и копий готовых форм тендерного предложения несет участник тендера.
  2. Оригиналы готовых форм тендерного предложения — это документы в сканированном виде, которые подписаны лицом (лицами), имеющим(и) полномочия выступать от имени субъекта на подписание договоров, и заверены печатью.
  3. Копии готовых форм тендерного предложения заполняются аналогично оригиналу и не должны содержать подписей, печатей, наименований, адресов, телефонов и иной информации, указывающей на принадлежность к Вашей фирме. **Данные документы присылаются в формате word или excel.**
  4. В тендерном предложении не должно быть никаких исправлений, добавлений между строчками, подтирок или приписок.

**Содержимое 1-го конверта:** Квалификационная информация (см. пункт 2.1.), рекомендации, отзывы, резюме и др. документы, перечисленные в Техническом задании, кроме заполненных готовых форм (Готовая форма №1 и Готовая форма №2 – «Финансовое предложение»);

**Содержимое 2-го конверта:**

1. Готовая форма № 1 с печатью и подписью лица, имеющего полномочия подписывать договоры и тендерные документы **- в 1 (одном) экземпляре.**
2. Готовая форма №1 без идентификации фирмы-участницы (без названия, печати и подписи фирмы-участницы) – **в 1 (одном) экземпляре.**

**Содержимое 3-го конверта:**

1. Готовая форма № 2 (Финансовое предложение) с печатью и подписью лица, имеющего полномочия подписывать договоры и тендерные документы **- в 1 (одном) экземпляре.**
2. Готовая форма №2 (Финансовое предложение) без идентификации фирмы-участницы

(без названия, печати и подписи фирмы-участницы) – **в 1 (одном) экземпляре.**

Участник также представляет любые другие документы, которые Участник должен будет заполнить или подготовить в соответствии с требованием Покупателя. Данные документы могут быть запрошены как во время тендера, так и после его проведения в рамках работы с победителем.

* 1. Неполное представление запрашиваемой информации или же подача тендерного предложения, не отвечающего всем требованиям, изложенным в технической спецификации тендера и настоящей Инструкции, может привести к отказу от предложения Покупателем.

Внимание! Все три конверта должны быть помеченными номерами 1, 2, 3.

1. **Право покупателя принять любую тендерную заявку и отклонить все тендерные заявки.**
   1. Покупатель оставляет за собой право принять или отклонить любую тендерную заявку, а также отклонить все тендерные заявки и аннулировать процесс тендера в любой момент до определения победителя, не неся при этом никаких обязательств перед участниками и не будучи обязанным информировать участника или участников о причинах таких действий.
   2. Покупатель оставляет за собой право отклонить тендерную заявку участника, имеющего какие-либо невыполненные обязательства перед Покупателем, имевшего судебные разбирательства с Покупателем и иным требованиям, не удовлетворяющим Покупателя.

|  |  |  |
| --- | --- | --- |
|  | **ПРИЛОЖЕНИЕ №1 ГОТОВАЯ ФОРМА № 1 (КОНВЕРТ №2)** | |
|  |  |  |
|  |  |  |
| **Квалификационные данные участника** | | |
| **№** | Квалификационное требование | Данные участника |
| **1** | Место регистрации компании |  |
| **2** | Основной Вид деятельности |  |
| **3** | Условия оплаты |  |
| **4** | Отсутствие незавершенных долговых обязательств, включая обязательства перед ГНС, СФКР и текущих судебных тяжб. |  |
| **5** | Срок поставки |  |
| **6** | Соответствие техническому заданию |  |
| **7** | Предоставление авторизационного письма от производителя ПО (MAF) **(с переводом на русский язык)** |  |

**ПРИЛОЖЕНИЕ №2 ГОТОВАЯ ФОРМА № 2 (КОНВЕРТ №3)**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |
| **№** | **Наименование** | **кол-во** | **стоимость, сом** | | **Примечание** |
| **за ед.** | **всего** |  |
| 1 | Fortify SCA Static Code Analyzer (SAST) | 1 |  |  |  |
| 2 | Fortify WebInspect (DAST) | 1 |  |  |  |

*Внимание: для резидентов* ***Цены указываются в национальной валюте Кыргызской Республики (сомах) с включением всех налогов.***

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

# Общие требования к Платформе

Лицензионное программное обеспечение (далее – ЛПО, Система) предназначено для статического сканирования и анализа имеющегося исходного (программного) кода (SAST) на наличие в нем ошибок и уязвимостей информационной безопасности, а также для анализа найденных потенциальных угроз. Система должна также поддерживать функционал динамического (DAST) сканирования приложений от того же производителя. Должна обеспечиваться возможность загрузки результатов Статического и Динамического сканирований на центральный сервер и их агрегирование в случае одного и того же приложения.

1. Общие требования к программному обеспечению для статического и динамического тестирования безопасности приложений
   1. Общие требования к программному обеспечению в части статического тестирования безопасности приложений
      1. Проведение статического анализа для поиска уязвимостей в исходном коде, написанном на следующих языках и фреймворках:
         * + ABAP/BSP;
           + Angular;
           + Flex/ActionScript;
           + ASP.NET, VB.NET, C# (.NET);
           + Apex;
           + .NET (Xamarin)
           + .NET Core
           + C/C++;
           + Classic ASP (VBs);
           + COBOL;
           + Cold Fusion;
           + Go
           + Kotlin
           + HTML;
           + Java (включая Android);
           + JavaScript/AJAX (ECMAScript 2015, 2016, 2017);
           + JSP J2EE;
           + MXML (Flex);
           + Objective-C/C++;
           + PHP;
           + Scala;
           + PL/SQL;
           + T-SQL;
           + Python 2/3;
           + Ruby;
           + Swift;
           + VB.NET;
           + Visual Basic 6;
           + VBScript;
           + XML.
      2. Решение должно иметь возможность проверки конфигурационных файлов докер контейнеров (docker container configuration files)
      3. Должно обеспечиваться определение кода в котором возникла уязвимость с трассировкой вызовов;
      4. Должно обеспечиваться предоставление описания механизмов эксплуатации для каждого типа уязвимостей
      5. Должно обеспечиваться предоставление рекомендаций по устранению для каждого типа уязвимостей;
      6. Обязательным требованием является интеграция с платформой контекстного обучения пользователей (возможность получить интерактивное обучение по найденной уязвимости и способам устранения)
      7. Должно обеспечиваться регулярное обновление базы уязвимостей, правил обнаружения уязвимостей.
      8. Решение должно разворачиваться на площадке заказчика, передача данных по сканируемым проектам производителю ПО не допускается;
      9. Предлагаемое решение должно присутствовать в международных рейтингах, например, Gartner Magic Quadrant for Application Security Testing или аналогичных. Лидерские позиции в таких рейтингах будут преимуществом.
      10. Решение должно позволять проводить статический анализ как минимум десять приложений и не должно накладывать ограничений на размеры приложений и количество поддерживаемых языков (должны поддерживаться тесты всех требуемых настоящим ТЗ языков). Количество персонала, которое допущено к проверке и просмотру результатов сканирования не должно быть ограничено. Динамический анализ не должен иметь ограничений в области количества проверяемых приложений/ проектов;
      11. Срок использования ПО – не менее 1 года. Минимальный срок технической поддержки - 12 месяцев в режиме 24\*7
   2. **В программном обеспечении должны быть реализованы следующие основные функции:**
      1. Функция настройки сканирования исходного кода приложения;
      2. Анализ исходного кода приложения;
      3. Анализ мультиязычных проектов с автоматическим распознаванием языков;
      4. Возможность обнаружения уязвимостей, связанных с ошибками разработчика;
      5. Поддержка обнаружения уязвимостей, связанных с намеренными действиями разработчика;
      6. Возможность проведения анализа байткода;
      7. Возможность проведения быстрого поверхностного сканирования;
      8. Конструктор правил для анализа исходного кода приложения;
      9. Группировка выявленных в исходном коде уязвимостей по типам таким как указано ниже.

Группировка выявленных в исходном коде уязвимостей согласно регламентам и категориям:

* + - * GDPR;
      * OWASP Top 10;
      * MISRA C/C++;
      * PCI;
      * SANS;
      * NIST;
      * STIG;
      * DISA;
      * CWE;
      * Новые уязвимости;
      * Принадлежность к пакету;
      * Принадлежность к файлу;
      * По точке утечки;
    1. Приоритезация выявленных и сгруппированных уязвимостей по степени критичности;
    2. Указание строки исходного кода, в которой выявлена уязвимость;
    3. Автоматическое формирование плана воспроизведения идентифицированной уязвимости с возможностью навигации по исходному коду приложения (построчно);
    4. Описание выявленной уязвимости в исходном коде и рекомендации по её устранению;
    5. Функция исключения выявленной уязвимости исходном коде из отчета;
    6. Функция добавления выявленных вручную уязвимостей c указанием строки кода;
    7. Формирование файла отчета с выявленными уязвимостями в форматах:
       - PDF;
       - HTML;
       - DOC;
       - XLS.
    8. Формирование файла отчета с выявленными уязвимостями на соответствие стандартам:
       - CWE/SANS top25;
       - DISA STIG;
       - PCI DSS;
       - FISMA Compliance: FIPS-200;
       - OWASP Top 10.
    9. Интеграция с системами постановки задач и контроля:
       - Jira;
       - Bugzilla;
       - Microsoft Team Foundation Server;
       - VSTS;
       - Micro Focus ALM.
    10. Функция интеграции с комплектами средств разработки:
        - IOS SDK;
    11. Функция интеграции со средами разработки:
        - Eclipse;
        - IntelliJ IDEA;
        - Android Studio;
        - WebStorm;
        - Visual Studio 2013 Premium, Professional, and Ultimate
        - Visual Studio 2015 Premium, Professional, and Ultimate
        - Visual Studio 2017 Community, Professional, and Enterprise;
    12. Функция интеграции с платформами сборки проектов:
        - Ant;
        - Gradle;
        - Maven;
        - MSBuild;
        - Xcodebuild;
        - Visual Studio (devenv).
    13. Функция интеграции с неподдерживаемыми напрямую инструментами сборки;
    14. Функция модульного сканирования исходного кода проекта
    15. Функция интеграции с платформами CI, включая плагины:
        - Bamboo;
        - Jenkins;
        - С любыми другими посредством CLI
    16. Функция повторного сканирования исходного кода приложения на предмет исправления ранее выявленных уязвимостей;
    17. Функция распараллеливания операции сканирования по потокам для оптимизации производительности;
    18. Возможность загрузки результатов статического анализа в единую серверную платформу управления тестированием безопасности программного обеспечения;
    19. Возможность бесшовной интеграции с решениями компании Sonatype для одновременного проведения статического анализа исходного кода на уязвимости и анализа open-source библиотек на наличие известных уязвимостей
    20. Должна поддерживаться опциональная возможность интеграции с решениями по анализу уязвимостей использующихся открытых библиотек. Результаты сканирования должны предоставляться в едином интерфейсе, как обобщение с результатами сканирования исходного кода.
    21. Производитель должен иметь возможность обеспечить наличие сервиса Статического (SAST) и Динамического (DAST) сканирования на удаленном сервере, с возможностью интегрировать сканирование в конвейер разработки и привлечением экспертизы производителя для проверки результатов. В случае дополнительного использования данной услуги необходимо наличие возможности выгрузки результатов сканирования с удаленного сервера производителя в локальную систему заказчика, с целью дальнейшего аудита и работы локально.
  1. **Требования к структуре и функционированию программного обеспечения статического анализа**

|  |  |  |
| --- | --- | --- |
| Операционная система | Архитектура | Платформа |
| Windows | 64-bit | Windows Server 2016/Windows Server 2012 R2/ Windows 8.1, 10 |
| Linux | 64-bit | Red Hat Enterprise Linux 6 update 5 и позжеRed Hat Enterprise Linux 7.x SUSE Linux Enterprise Server 12 |
| Oracle Solaris | x86, 64-bit | 10.5 и позже |
| Oracle Solaris | SPARC 64-bit | 10.5 и позже |
| Mac OS |  | 10.12, 10.13 |

* + 1. Программное обеспечение для статического тестирования безопасности приложений должно поддерживать операционные системы следующих версий:
    2. Программное обеспечение для статического тестирования безопасности приложений, работающее под управлением операционных систем Windows и Mac OS должно состоять из следующих основных компонентов и иметь графический интерфейс для каждого из них:
       - Помощник настройки сканирования исходного кода приложения;
         * Помощник настройки сканирования должен предоставить пользователю возможность выбора сразу несколько папок с исходными кодами приложения в рамках одного сканирования.
         * Помощник настройки сканирования исходного кода приложения должен автоматически определять языки программирования, на которых написано приложение;
       - Конструктор собственных правил сканирования исходного кода приложения;
         * Правила, созданные в конструкторе собственных правил сканирования исходного кода приложения, должны иметь возможность подключения к помощнику настройки сканирования для применения их во время сканирования исходного кода.
       - Консоль анализа выявленных уязвимостей и формирования отчетов;
         * Консоль анализа выявленных уязвимостей и формирования отчетов должна предоставлять подробную информацию по выявленным уязвимостям, группировать их по типам и приоретизировать их в автоматическом режиме;
         * В консоли анализа выявленных уязвимостей и формирования отчетов должна быть предусмотрена фильтрация выявленных уязвимостей по уровню опасности и типам;
         * В консоли анализа выявленных уязвимостей и формирования отчетов должна быть реализована возможность для ручного отбора и исключения из отчета выявленных уязвимостей;
         * В консоли анализа выявленных уязвимостей и формирования отчетов должна быть реализована подсветка строки кода с выявленной уязвимостью, её описанием и рекомендациями по устранению;
         * В консоли анализа выявленных уязвимостей и формирования отчетов должна быть реализована возможность подключения к системе постановки задач и контроля и заведение в ней задачи по выявленной уязвимости;
         * В консоли анализа выявленных уязвимостей и формирования отчетов должна быть реализована возможность заведение задачи по выявленной уязвимости в системе постановки задач и контроля в ручном и автоматическом виде.
         * В консоли анализа выявленных уязвимостей и формирования отчетов при формировании отчета должна быть реализована возможность выбора формата файла отчета и шаблона.
  1. **Требования к единой серверной платформе управления тестированием безопасности программного обеспечения.**

Система должна выполнять функции:

* + 1. Интеграции с системами багтрекинга индивидуально по каждому приложению или команде
    2. Поддержки процесса управления уязвимостями
    3. Поддержки дашбордов по приложениям
    4. Объединения в единое представление результатов статического и динамического анализа
    5. Синхронизации и объединения результатов машинного сканирования и работы экспертов по анализу результатов
    6. Предоставления возможностей выполнения ручного анализа кода по каждой потенциальной уязвимости аналогично функционалу модуля статического анализа
    7. Возможность интеграции в SSO
    8. Возможность аутентификации пользователей по AD/LDAP
    9. Наличие war образа для развертывания на стандартном сервере приложений
    10. Наличие Kubernetes образа для развертывания в промышленной среде контейнеризации для всех компонент решения.
    11. Иметь Мастер по созданию shell и bat скриптов сканирования с возможностью кастомизации и выбора опций сканирования и дальнейшей обработки результата.
    12. Иметь возможность добавить дополнительный модуль анализа для идентификации и классификации потенциальных уязвимостей на ложные и реальные с весовым коэффициентом на базе машинного обучения, с возможностью обучать в том числе на своем коде.
  1. **Общие требования к программному обеспечению в части динамического тестирования безопасности Web-приложений**
     1. Результаты динамического сканирования приложений должны дополнять результаты статического тестирования их исходного кода. Результаты должны быть представлены в единой среде для удобства анализа.
     2. Решение должно разворачиваться на площадке заказчика, передача данных по сканируемым проектам производителю ПО не допускается
     3. Решение должно позволять проводить динамический анализ неограниченного количества приложений/проектов.
     4. Решение должно позволять идентифицировать уязвимости в работающих Web-приложениях, как наследуемых, так и приложениях собственной разработки. Эвристические механизмы должны обнаруживать большинство типичных ошибок, допускаемых при разработке Web-приложений: внедрение операторов SQL (SQL Injection), межсайтовое выполнение сценариев (Cross-Site Scripting, XSS) и др.
     5. Должна предоставляться возможность составления дерева сайта;
     6. Должна предоставляться возможность организации fuzzy атаки с параметризацией по всем обнаруженным принимаемым приложениям данным;
     7. Решение должно логировать все атаки с возможностью просмотра трафика;
     8. Решение должно иметь возможность установки агента на сканируемое приложение, для сбора дополнительных подтверждающих данных о результатах атак;
     9. Решение должно поддерживать различные современные технологий, в т.ч. – HTML5, JSON, Adobe Flash, Ajax, SOAP и другие. Помимо обнаружения уязвимостей, решение должно также помогать устранять уязвимости, и должно предоставлять доступ к базе знаний, в которой приводятся не только описания уязвимостей и возможностей их использования, но и рекомендации по устранению уязвимостей.
     10. Решение должно обеспечивать простое развертывание и масштабирование при необходимости сканирования значительного количества Web-приложений.
     11. Решение должно позволять с легкостью формировать отчеты для Руководства (статистика уязвимостей, общие показатели и т.п.), а также создавать заключения для разработчиков (сведения о каждой уязвимости и приоритетность исправлений).
     12. Решение должно позволять проверять на уязвимости REST – сервисы, документированные на базе Swagger или с помощью Postman коллекций.
     13. Решение должно позволять проверять на уязвимости ODATA API
     14. Решение должно позволять проверять на уязвимости SOAP сервиса