Техническое задание на организацию и проведение комплексных мероприятий по безопасной разработке (AppSec) для сотрудников холдинга

# **Цель закупки и задачи, которые должен решать**

Цель закупки: Организация и проведение мероприятий, нацеленных на формирование у сотрудников команд разработки навыков по обеспечению безопасности разработки (AppSec), предотвращению появления уязвимостей в продуктах холдинга, а также развития технических компетенций сотрудников в роли Security Champions. Предполагаемое количество сотрудников от 50 до 250 в каждом CTF.

Проведение комплексных мероприятий призвано решать следующие задачи:

1. Минимизирование дефектов информационной безопасности и безопасности приложений (AppSec) в разрабатываемых программных продуктах.
2. Снижение стоимости исправления дефектов информационной безопасности программного обеспечения за счёт своевременного повышения безопасности кода благодаря приобретённым компетенциям сотрудников.
3. Комплексное обучение команд безопасной разработке мобильных и веб приложений, а также отработка полученных знаний на практике
4. Формирование внутреннего центра компетенций AppSec, аккумулирующего экспертизу в области безопасной разработки.
5. Обучение принципам работы с дефектами.

# **Требования к квалификации поставщиков**

Поставщики должны иметь:

- опыт организации и проведения соревнований по захвату флага CTF (Capture the Flag) для Android, iOS и веб уязвимостей;

- опыт разработки материалов и интерактивных тренажёров по безопасности приложений (AppSec)

- при разработке материалов и мероприятий должны принимать участие эксперты и авторы программ являются действующими сотрудниками компаний-лидеров в области кибербезопасности и AppSec, имеют общий стаж преподавания не менее 2 лет, а также обладать сертификатами и документами, подтверждающими высокий уровень экспертизы в области ИБ и AppSec

- успешный подтвержденный опыт организации и проведения мероприятий по теме AppSec

# **Требования по организации и проведению комплексных мероприятий AppSec для сотрудников**

*Таблица 1: Требования*

|  |  |  |
| --- | --- | --- |
| **Название блока** | **Объем** | **Требования к содержанию блока** |
| CTF (англ. Capture the flag) — соревнования по обнаружению уязвимостей в приложениях | 6 недель (3 события, до 2 недель на каждое) | Соревнования организуются в формате классического Jeopardy/task-based, когда на каждое задание в рамках соревнования есть собственный флаг. Темы заданий – наиболее часто используемые злоумышленниками уязвимости приложений (Web, Android, iOS).  Всего в рамках каждого CTF запланировано порядка 15-20 интерактивных заданий, покрывающих поверхность атаки потенциального злоумышленника. |
| Подготовка сотрудников к CTF по уязвимостям приложений | До 18 ак. часов (по 6 ак.часов на соревнование) | Подготовка сотрудников к соревнованиям по поиску уязвимостей в приложениях проходит в формате онлайн-вебинара или очного мероприятия. Нужна возможность задавать вопросы преподавателю, ведётся видеозапись мероприятий, минимум одно событие (от 2 ч.) должно быть очным в Москве, с проведением фотосъёмки процесса.  В рамках мероприятий на практических примерах разбираются основные уязвимости приложений, которые будут отработаны в рамках CTF    Темы при подготовке **не должны** дублировать список ниже, исполнителю необходимо предложить **новое** содержание, в дополнение к нему:  1. Статический анализ приложения (Web, Android, iOS):  - Декомпиляция приложения  - Дизассемблирование приложения  - Работа с бандлом приложения  - Поиск секретов  - Проверка секретов сторонних сервисов  - Поиск ключевых хранилищ и их анализ  2. Анализ приложения во время работы (Web, Android, iOS): - Подходы к Jailbreak, обход Jailbreak  - Анализ файловой системы устройства  - Анализ журнала системы  - Анализ применяемых методик шифрования - Динамическая инструментация приложений  - Фреймворки Frida, Objection   3. Сетевое взаимодействие (Web, Android, iOS): Анализ взаимодействия серверной части и клиентского приложения  Способы перехвата трафика  Принципы защиты и способы обхода данной защиты  4. Ошибки клиентской части (Web, Android, iOS):  Межпроцессное взаимодействие  Переполнения и защита от них  Биометрическая аутентификация  Использование Security Enclave |
| Воркшопы по итогам CTF по обнаружению уязвимостей приложений | 6 ак.часов  (3 события по 2 ак часа) | В рамках воркшопов будет продемонстрировано решение задач CTF, осуществлен разбор ошибок, по итогам будут предоставлены подробные решения (write-up) для задач CTF |
| Интерактивный тренажёр для подготовки к соревнованиям CTF – для практического закрепления навыков, полученных при подготовке | Один интерактивный тренажёр, передаваемый на сторону заказчика – практика до 20 ак.часов | Интерактивный тренажёр может быть представлен в виде SCORM-пакета с тестами. Темы в тренажёре **не должны** дублировать список ниже, исполнителю необходимо предложить **новое** в дополнение к нему:   * Главные угрозы безопасности приложений. OWASP Top 10 * Методические подходы к безопасности приложений * Основные практики DevSecOps * Основные практики безопасной разработки AppSec и Pentest * Модель бизнес-процессов * Основы безопасности веб-приложений * OWASP Top 10 * Браузерные и серверные механизмы защиты * Инъекции * Использование компонентов с известными уязвимостями * Основы безопасности (аутентификация, идентификация, хэширование) * Безопасность приложений на платформе Android * Угрозы Android Некорректное использование платформы Небезопасное хранение данных * Небезопасная передача данных * Небезопасная аутентификация * Использование слабой криптографии * Небезопасная авторизация * Низкое качество и модификация исходного кода * Reverse Engineering * Скрытая функциональность * Безопасность iOS-приложений * Недокументированная функциональность |

# **Требования по организации и проведению мероприятий**

4.1 Проведение соревнований

Не менее 1 недели, не более двух недель

4.2 Наличие платформы для проведения соревнований со стороны поставщика

4.3 Наличие динамического скоринга в соревнованиях

4.4 Задания для проведения

Распределение задач по 3 уровням сложности: простые, средние и сложные

4.5 Наличие технической и организационной поддержки до и во время проведения соревнований

4.6 Наличие возможности изготовления брендированных призов для победителей соревнований

4.7 Наличие возможности редизайна платформы провайдера под стилистику компании

4.8 Наличие возможности провести минимум одно событие в рамках таблицы в блоке 3 – в очном формате в Москве, с привлечением фотографа со стороны исполнителя

4.9 Наличие возможности передать заказчику в бессрочное пользование видеозаписи подготовительных мероприятий, фотоматериалов, а также интерактивных тренажёров

# **Сроки предоставления услуг**

Предоставление – 2 квартал 2025 года

# **Форма оплаты услуг**

Предлагается участником.