«ПОДТВЕРЖДАЮ»
АКБ «Банк развития бизнеса»
Заместитель председателя правления:
Б.Бобожонов

«26» август 2025 г.
№ 179

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

«Программный комплекс управления уязвимостями в информационно-телекоммуникационной среде»

Ташкент 2025г.

Технические требования

Функциональные требования	
Программный комплекс управления уязвимостями в информационно-телекоммуникационной среде	
Общие системные требования	Система должна иметь возможность поставки, включая, но не ограничивая, в виде следующих вариантов: - Готового виртуального устройства (VA - Virtual Appliance) для VMware или Hyper-V; - Пакета установки на ОС Linux. Система должна обеспечивать возможность сканировать не менее 500 IP адресов и 5 FQDN в ИТС.
Центральное управление	Система должна обеспечивать централизованное управление всеми её компонентами и функционалом через единый Веб-интерфейс. Система должна сохранять результаты сканирований и оценки активов в базе данных для возможности построений отчетов и хронологии изменений. База данных должна соответствовать следующим критериям: - Не требовать использования сторонних БД для сохранения результатов Обеспечивать раздельное хранение данных сканирования в репозиториях в зависимости от результата (типы уязвимостей, группы ресурсов и пр.), при анализе или запросе данных комбинировать результаты в любой комбинации Хранить данные заданный и настраиваемый период времени, после истечения которого автоматически очищать базу данных (БД) от устаревшей информации.
Пользователи системы	Система должна поддерживать управление на основе ролей и разграничение прав доступа: • Обновление проверок базы данных; • Выполнение любого сканирования, при условии наличия политики сканирования или отсутствии ее; • Управление пользователями; • Доступ к просмотру данных об уязвимостях; • Определение, создание и предоставление совместного использования списков активов; • Добавление файлов аудита; • Создание оповещений; • Определение и совместное использование учетных данных

	для сканирования с предоставлением учетных данных; • Создание и совместное использование политик сканирования; • Управление билетами (Workflow); • Аудит пользовательских действий. Система должна позволять пользователю принять риск обнаруженной уязвимости или переопределить до необходимого уровня, не зависимо от определенного поставщиком. Система должна поддерживать управление билетами рабочих процессов для расследований и устранения уязвимостей. Система должна позволять назначать билеты персонально. Система должна поддерживать список уязвимостей, которые относятся к билету. Система должна предоставлять возможность пользователю настраивать базовые параметры безопасности и доступа к платформе, такие как: 🕐 Парольную политику; 🕐 Таймаут сессии. Система должна предоставлять возможность создания неограниченного количества пользователей Системы.
Шифрование передаваемых данных	Система обязана шифровать коммуникации между компонентами/модулями Системы. Система должна обеспечивать шифрование коммуникации между пользователями и Системой.
Поддержка внешней аутентификации и авторизации	Система должна интегрироваться с системами сторонних производителей (LDAP, AD) для обеспечения аутентификации и авторизации внутренних пользователей.
Производительность системы	Система должна обеспечивать возможность сбора и анализа, аудита с коммутационного оборудования, маршрутизаторов, межсетевых экранов и систем предотвращения вторжений. Хранить полученные события, уязвимости, отчеты не менее 999 дней.
Управление активами	Система не должна полагаться на внешние сканеры для обнаружения активов, сканирования портов или идентификации ОС. Система должна иметь возможность без использования активного, либо агентского сканирования, на основании разбора трафика, определять появление новых активов в сети. При этом система как минимум должна идентифицировать активы по следующим типам:

	Сервера Рабочие станции Приложения Операционные системы Сетевые устройства Виртуальные и облачные системы BYOD устройсва Мобильные телефоны Устройства с взломанной iOS Система должна иметь возможность неограниченного инвентаризационного сканирования сети как по расписанию, так и по требованию. Система должна уметь связывать результаты сканирования с активами в DHCP-среде, где IP-адреса могут изменяться. Система должна иметь возможность ручного группирования активов на основании различных критериев и правил. Система должна иметь встроенный функционал автоматической классификации и динамической маркировки определенных активов в сети, включая, но не ограничивая следующие критерии: По принадлежности к IP подсети; На базе NetBIOS и FQDN имени; На базе операционной системы; По открытым портам/сервисам; По наличию конкретной уязвимости; На основании сроков сканирования; Активы, которые пропустили сканирование по расписанию и т.д. Система должна позволять настраивать нагрузку на инфраструктуру, во избежание перегрузки каналов заказчика во время проведения задач сканирования Система должна автоматически запускать службы удаленного реестра на системах Windows при выполнении сканирований с предоставлением прав, а затем автоматически останавливать эти службы после того, как сканирование завершено.
Поддерживаемые ОС и БД для сканирования	Система должна поддерживать, включая, но не ограничивая сканирование следующих операционных систем: • Microsoft Windows; • AIX;

	• Solaris; • HP/UX; • Linux; • Netware; • MacOS. Система должна поддерживать, включая, но не ограничивая сканирование следующих баз данных: 🕐 MS SQL; 🕐 IBM DB2; 🕐 Informix/DRDA; 🕐 MySQL; 🕐 Oracle Database; 🕐 PostgreSQL; 🕐 Sybase ASE.
Визуализация данных (Dashboard)	Система должна иметь встроенный набор панелей для визуализации данных (Dashboard). Система должна позволять создавать пользовательские панели визуализации данных. Панели визуализации должны иметь функцию автоматического обновления. Система должна поддерживать «drill-down» элементов панели визуализации в отдельное окно (для реализации непрерывного мониторинга, расследования инцидентов). Система должна поддерживать предоставление общего доступа к панелям визуализации данных. Панели визуализации должны позволять фильтровать информацию с помощью выбора, тэгов, активов, времени и пр. Система должна позволять создавать выгружать отчеты на основе отображаемых панелей визуализации данных.
Поддержка API	Система должна предоставлять API для доступа к информации, находящейся в базе данных системы. Система должна иметь API для возможности интеграции с другими системами API должно быть предоставлено бесплатно.
Автоматическое обновление	Система должна обеспечивать автоматическое обновление конфигураций без дополнительных временных затрат со стороны пользователя системы. Например, обновление баз уязвимостей по отдельным компонентам системы. Автоматическое обновление должно включать, но не

	ограничиваться следующим: • Обновление по расписанию; • Обновление в ручном режиме; • Возможность загрузить обновление и установить в необходимый период.
Резервное копирование и восстановление	Система должна обеспечивать автоматическое резервное копирования конфигурации и возможность восстановления конфигурации с резервной копии из графического единого веб-интерфейса. Система должна иметь возможность хранить копию конфигурации отдельно от решения.
Масштабирование	Система должна обеспечить простое, быстрое масштабирование и расширение функционала без необходимости дополнительных инвестиций со стороны купленного функционала. Система должна обеспечить взаимодействия географически отдаленных модулей, без дополнительных затрат на обслуживание. Система должна поддерживать балансировку нагрузки, восстановление после сбоя на сканерах уязвимости путем динамического распределения нагрузки между сканерами на основании наличия сканера на протяжении всего задания сканирования.
Сканирование	Система должна реализовывать возможности: • Сканировать по расписанию; • Включать/отключать необходимые тесты в заданных задачах сканирования; • Приостановить задачу на необходимое время; • Иметь возможность автоматически исключить критические ресурсы из сканирования, если они заняты служебными процессами, согласно расписанию; • Сканирование изолированного сегмента сети и последующей выгрузкой результатов в единую консоль; • Выбор уязвимостей для сканирования; • Сканирование определённых портов; • Использование учётных записей. Система должна иметь возможность при сканировании выполнять как минимум следующие типы аутентификации: • Для OS Windows: логин и пароль, Kerberos, CyberArk Vault, Lieberman, Thycotic Secret Server, Arcon, Centrify, BeyondTrust, Hashicorp Vault, NTLM Hash, LM Hash; • Для Unix систем: логин и пароль, Kerberos, CyberArk Vault, Lieberman, Thycotic Secret Server, Arcon, Centrify, BeyondTrust,

	Hashicorp Vault, Certificate, Public Key; • Для сетевого оборудования – SNMP; Система должна иметь возможность принимать цели сканирования в разных форматах: активами, IP адресам, IP сетям, именами. Сканирующий модуль должен устанавливаться как минимум на следующие операционные системы: • Windows; • MacOS; • Amazon Linux 2; • Red Hat Enterprise Linux; • Fedora. Система должна позволять пользователям писать и использовать собственные проверки при сканировании. Система должна включать в себя возможность для пассивного сканирования уязвимостей путем наблюдения сетевого трафика на уровне пакетов, без активного сканирования систем для сетей ipv4 и ipv6. При этом система должна определять, как минимум: • Взаимодействие между активами в инфраструктуре; • Список используемых портов; • сканирование портов, выполняемое сторонними системами; • Тип зашифрованых и не зашифрованых сетевых сеансов; • Передачу конфиденциальной информации без использования шифрования; • уязвимости в коммуникационных системах; • уязвимости в используемых протоколах; • уязвимости в приложениях. Функционал Системы по обнаружению уязвимостей веб-приложений (DAST) должен выполнять: • Сканирование Веб-приложений на наличие уязвимостей с использованием авторизации или без нее; • Указание на ошибки конфигурации; • Выполнение сканирования REST API на наличие уязвимостей; • Проведение ssl/tls аудита Система должна иметь возможность сканирования Веб-приложений на распространенные уязвимости веб-приложений таких как: SQL injection, cross-site scripting (XSS), HTTP header injection, directory traversal, remote file inclusion, command

	execution. Для найденных уязвимостей должна применяться градация по OWASP TOP 10.
Идентификация уязвимостей	Система должна обнаруживать и классифицировать проблемы, риски и уязвимости. Также должна предоставить подробную информацию о характере риска и рекомендаций по их минимизации. Система должна сообщить об известных уязвимостях в активе которые должны быть определены консультативными организациями в области безопасности (например, Common Vulnerabilities and Exposures database (CVE) или Common Weakness Enumeration (CWE) или The SecurityFocus Bugtraq (BID) или любой комбинацией из них). База Данных уязвимостей продуктов должна включать проверки: OS Security and Patch; CISCO; Firewalls; DNS; FTP; SMTP; RPC; SNMP; LDAP; SMB; CGI; Web Servers; Databases; Backdoors; Denial of Service; Default Accounts; Peer-To-Peer; Remote Shell; Система должна иметь возможность: • обнаружения сервисов, которые выполняются на нестандартных портах. • обнаружения сервисов не настроенных на отображение баннеров подключения. • тестировать несколько экземпляров одного и того же

	сервиса, работающих на разных портах. • сканировать «мертвые узлы» (устройства, которые не отвечают на команду «ping»).
Аудит	Система должна предоставить возможность производить аудит конфигурации и наличия исправлений в системах Windows и Unix/Linux. Система должна предоставить политики аудита для Windows, Unix/Linux, приложений, Cisco устройств, баз данных, с возможностью использования пользовательских конфигураций.
Приоритезация	Система должна иметь возможность дополнительной интеллектуальной приоритизации, с помощью которой система должна определять приоритеты уязвимостей на основе вероятности того, что каждый из них будет использован во время атаки и сочетать в себе независимые источники данных, включая данные об уязвимостях производителя и сторонние данные об уязвимостях и угрозах , используя собственный алгоритм машинного обучения для выявления уязвимостей с наибольшей вероятностью эксплуатации в ближайшем будущем. Данная функциональность должна работать внутри системы без необходимости подключения к сети Интернет.
Оповещения и уведомления	Система должна поддерживать оповещения на основании результатов сканирования уязвимостей или аудита конфигураций. Действия уведомлений должны включать в себя: Настраиваемые почтовые адреса с возможностью использовать переменные контекста: 🕐 Создание билетов; 🕐 Начать сканирование; 🕐 Пересылка Syslog события.
Отчетность	Система должна предоставлять отчетность по всем событиям, отчетность должна быть доступна через Веб-интерфейс. Система должна давать возможность самостоятельной настройки отчетности и создания собственных отчетов. Система должна иметь возможность генерации отчетов по запросу. Система должна предоставлять примеры сгенерированных отчетов для более простого использования и генерации новых отчетов пользователем. Система должна иметь встроенные отчеты. Система должна иметь встроенные, либо быстро доступные готовые пакеты отчетов лучших практик (NIST, CIS, ISO). Система должна предоставлять отчеты за определенный период времени по различным сегментам и системам в сети.

	Отчеты, формируемые системой, должны как минимум содержать следующую информацию: - Название уязвимости и уровень ее критичности по шкале вендора и по CVSS; - Перечень уязвимых систем или сервисов; - Статус уязвимостей; - Рекомендации по устранению уязвимости, или ссылку на патч, если таковой существует; - Дополнительные критерии для приоритизации уязвимости: наличие эксплойта, вредоносного кода, и тд.
Управление уязвимостями	Система должна отслеживать дату обнаружения уязвимости и дату последнего обнаружения для фильтрации и формирования отчетов по времени нахождения уязвимости в инфраструктуре. Система должна поддерживать проверку отсутствия исправлений, наличие сервисов, проверки соответствия файлам аудита и другие. Система должна предоставить возможность сканировать ресурсы внутри, вне сети с использование агентов, при необходимости без агентов.
Разведка угроз	Система должна предоставлять возможность просматривать информацию о известных уязвимостях, информация о которых должна поступать из базы данных производителя. База данных производителя должна основываться на таких источниках, как внутренняя экспертиза, рекомендации поставщиков, консультативная база данных GitHub и Национальная база данных уязвимостей. Система должна предоставлять категоризацию уязвимостей, которая сочетает известные показатели риска с выводами исследовательской группы производителя для выявления наиболее важных уязвимостей. Функционал категоризации уязвимостей должен предоставлять возможность разбивать ключевые уязвимости из базы данных производителя на категории, включая, но не ограничиваясь следующими категориями: - Emerging Threats; - Recently Actively Exploited; - Ransomware; - In the news. Система должна предоставлять возможность: - поиска в базе данных уязвимостей производителя; - профилизации уязвимостей; - сравнения уязвимостей Организации с известными

	уязвимостями. Поиск в базе данных уязвимостей производителя должен предоставлять возможности поиска по CVE ID. Профиль уязвимости должен предоставлять возможность детального анализа уязвимости и включать временную шкалу событий, активы в инфраструктуре и продукты, которые пострадали, источники происхождения и показатели, такие как профиль риска и серьезность. Функционал сравнения уязвимостей должен предоставлять возможность сравнивать список уязвимостей из определенной категории с выявлениями в среде.
Возможности расширения	Система должна иметь возможность расширения функционала путем добавления приложений с официального сайта производителя. Система должна иметь возможность расширения функционала путем добавления пассивного сканера, для поиска уязвимостей, того же производителя. Пассивный сканер должен обеспечивать возможность пассивного сканирования уязвимостей путем наблюдения сетевого трафика без активного сканирования системы.
Лицензирования	Лицензирования системы должно проходить по количеству IP, не зависимо от лицензирования отдельных компонентов системы. В лицензию должны быть включены: - Не лимитированное количество сканеров; - Количество Agents равняется количеству IP-адресов; - Политики аудита системы на соответствие мировым стандартам (DISA STIG, CIS, MSCT и др.); - Rest API.
Интеграции	Система должна поддерживать интеграции со следующими решениями: - APCON - Network Monitoring; - Aruba, a Hewlett Packard Enterprise company – NAC; - Axonius – CMDB; - Atlassian - Security Operations; - BeyondTrust - Privileged Access Management; - BMC – Patch Management; - Brinqa – TVM; - Cisco – NAC; - CyberArk - Privileged Access Management; - Cymulate – Simulation;

	• Dell - Patch Management; • ForeScout – NAC; • Garland Technology – Networking; • Gigamon – Networking; • Good powered by Blackberry – MDM; • HCL BigFix - Patch Management; • IBM – SIEM; • Infoblox - IP Address Management; • Kenna – TVM; • LogRhythm - SIEM; • Microsoft – SIEM; • Red Hat - Patch Management; • Redseal – TVM; • ServiceNow - Security Operations; • Splunk – SIEM; • Symantec - Patch Management; • Thycotic - Privileged Account Management. Все перечисленные интеграции должны поддерживаться производителем Системы.
Развертывание	Все компоненты Системы должны иметь возможность устанавливаться и поддерживаться локально без необходимости подключения к сети Интернет Система должна поддерживать возможность активации оффлайн. Система должна поддерживать обновления Системы и информации об уязвимостях без необходимости подключения к сети Интернет.

1. Гарантия и сервисная поддержка оборудования

Оборудование должно обеспечиваться гарантией от производителя и сервисной поддержкой сроком не менее 12 месяцев.

Условия сервисной поддержки должны включать в себя возможность регистрации сервисных случаев в режиме 24x7x365, обновление микрокода системы и версий установленного программного обеспечения.

Дополнительные требования:

- Наличие инженера со знанием **узбекского и русского/английского языков** для взаимодействия с пользователями и ведения коммуникации по техническим вопросам.

2. Требования к Исполнителю

2.1. Квалификационные требования

Подтвердить участие в проекте со стороны Поставщика не менее 1 (одного) сертифицированного инженера от производителя, предоставив действующие сертификаты.

2.2. Прочие требования к Исполнителю

В рамках выделенного бюджета Исполнитель должен выполнить следующие требования:

- Поставка выполняется в полном объеме в адрес Заказчика (Представителя заказчика);
- Исполнитель должен предоставить письмо авторизации (Manufacturer Authorization Form, МАФ) от уполномоченного представителя производителя, подтверждающее право поставлять товар на территории Республики Узбекистан;

3. Требования к интеграционным работам и обучению

В состав предложения участника конкурса должно быть включено авторизованное обучение по всем программным продуктам– 2 сотрудника.

В состав поставки должны быть включены услуги по внедрению решения Системы управления уязвимостями для обеспечения информационной безопасности инженерами Поставщика.

4. Требования к документации проекта

В рамках выполнения работ Заказчику должны быть предоставлены Исполнителем нижеперечисленные документы:

- Техническая документация от производителя оборудования;
- Исполнительная документация проекта со включением отчета по тестированию
- Акт приемки в промышленную эксплуатацию.