**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 Qualys VMDR + PM.**

**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 | Qualys VMDR | 2000 |  |  |  |
| 2 | Qualys PM Windows | 1600 |  |  |  |
| 3 | Qualys PM Linux | 400 |  |  |  |
| 4 | Qualys Express Suite | 1 |  |  |  |

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

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

# Общие требования к Платформе

* Все модули Платформы должны иметь единый веб-интерфейс
* Модули Платформы должны быть интегрированы и обмениваться информацией между собой
* Во всех модулях должны быть единые настройки учётных записей
* Платформа должна предоставлять возможность пользователю настраивать базовые параметры безопасности и доступа к Платформе, такие как:
  + Парольную политику
  + Ограничение доступа по IP
  + Использование двухфакторной аутентификации
  + Журналирование действий
  + Таймаут сессии
* Платформа должна поддерживать SAML для процесса подключения к платформе
* Платформа должна предоставлять возможность отдельного независимого лицензирования всех модулей системы
* Платформа должна предоставляться в виде годовой (и более) подписки на доступ к облачному ПО (SaaS)
* Платформа должна предоставляться в виде подписки на сервис
* В стоимость платформы должно входить обучение сотрудников компании работе с системой (без ограничения по количеству человек). По результатам обучения сотрудники компании должны сдавать экзамен и получать сертификат. Должна быть возможность проведения обучения как в очном так и заочном (online) формате.
* В стоимость системы должна входить техническая поддержка 24/7/365
* Обновления сигнатур должны выходить на ежедневной основе
* Платформа должна предоставлять возможность создания неограниченного количества пользователей системы
* Для Платформы должна быть реализована возможность ролевого доступа пользователей, обеспечивающая как минимум:
  + Наличие суперпользователя, для администрирования всех аспектов работы платформы
  + Наличие ряда предустановленных ролей
    - Пользователь для запусков сканирований
    - Пользователь для запуска отчётности
    - Пользователь для получения уведомления от платформы
    - Пользователь для доступа к тикетам
    - И тд
  + Разграничение доступа пользователей к отдельным ресурсам
  + Разграничение доступа пользователей к различным компонентам системы
  + Возможность создания отдельных подразделений в рамках Платформы для ограничения доступа для групп пользователей
* Платформа должна обеспечивать возможность доступа через встроенный API ко всем модулям
* Платформа должна предоставлять возможность агентного и безагентного сбора информации
* Платформа должна покрывать в режиме управления уязвимостей – 2000 узлов (внешних и внутренних); в режиме контроля соответствия требованиям (compliance) – 2000 узлов; в режиме патч-менеджмент – 1600 узлов под управлением Windows, 400 узлов под управлением Linux, в режиме инвентаризации (в т.ч. контейнеров, облаков, мобильных устройств) – неограниченное количество узлов, и включать неограниченное количество сенсоров – прокси для агентов, сетевые сканеры, пассивные сенсоры, и пр.

# Требования к подсистеме агентского сбора информации

* Агент должен быть доступен для платформ на базе пользовательских версий Windows (начиная с версии Windows XP SP3), серверных версий Windows (начиная с Windows 2003), Linux, MacOS, AIX, FreeBSD, Solaris, Z-Linux
* Агент, независимо от режима работы, не должен выполнять обработку информации на стороне клиента. Он должен собирать информацию и передавать в Платформу для дальнейшего анализа
* Агент должен иметь возможность в разных режимах, как минимум: режиме инвентаризации, режиме сканирования на уязвимости, режиме проверки на соответствие требованиям, режиме поиска индикаторов компроментации (IOC), режиме контроля целостности файлов, режиме установки патчей
* В режиме инвентаризации агент должен собирать следующую информацию (как минимум):
  + Перечень установленного ПО
  + Перечень открытых портов
  + Сетевые интерфейсы
  + Сервисы
  + Базовую информация по железу (Процессор, Жёсткие диски, Оперативная память, производитель и тд)
  + Пользователи группы локальных администраторов и последний подключённый пользователь
  + Время запуска компьютера
* У пользователя Платформы должна быть возможность настраивать профили работы агентов, в том числе управлять следующими параметрами:
  + Использованием процессора
  + Параметрами подключения к Платформе
  + Нагрузкой на сеть при передаче информации
  + Частотой сбора информации
* По умолчанию Платформа должна обеспечивать автоматическое обновление агентов. У пользователя Платформы должна быть возможность управления обновлением агентов.
* Агент должен иметь возможность передавать информацию в платформу как напрямую, так и через прокси-сервер
* У Платформы должен быть свой прокси-сервер для агентов, позволяющий, как минимум:
  + Кэшировать траффик агентов
  + Кэшировать обновления (при использовании модуля установки обновлений)
  + Блокировать коммуникации агентов с любыми серверами, кроме серверов Платформы
* В Платформе должны быть предустановленные дэшборды для мониторинга состояния работы агентов

## Пассивный сканер

* Должен идентифицировать и категорировать различные IT устройства в потоке трафика.
* Должен предоставлять информацию о найденном устройстве, как минимум:
  + тип устройства
  + тип операционной системы
  + открытые порты
  + используемые сервисы
* Должен идентифицировать и категорировать используемые сервисы в потоке трафика.
* Должен предоставлять полную информацию о найденном сервисе, как минимум:
  + тип сервиса
  + используемый протокол
  + используемый порт
* Должен предоставлять информацию по трафику, как минимум:
  + IP адреса источника и назначения
  + Используемые порты источника и назначения
  + Используемый протокол
  + Тип сервиса
  + Объем переданного и принятого трафика
* Должен предоставлять информацию по трафику как в текстовом/табличном, так и в графическом виде
* Должна быть возможность поиска в информации по собранному трафику
* Информация по трафику должна обновляться в режиме реального времени
* Устройство для сбора трафика должно поставляться в виде виртуального сервера для гипервизора VMware ESXi
* Устройство для сбора трафика должно поддерживать обработку трафика до 1 Гбит/с

# Требования к модулю анализа защищённости инфраструктуры

## Общий функционал модуля анализа защищённости

* Возможность неограниченного инвентаризационного сканирования сети как по расписанию так и по требованию
* Возможность сканирования на уязвимости как с помощью агентов так и в безагентном режиме
* Возможность проведения сканирования сети на уязвимости как по расписанию так и по требованию
* Возможность проведения сканирования на соответствие стандарту PCI DSS по расписанию так и по требованию
* Предоставление доступа к базе уязвимостей, с описанием уязвимостей, а также с рекомендациями по их устранению
* Возможность сканирования на уязвимости периметра из датацентра Платформы
* Для безагентного сканирования должна быть возможность задавать профили сканирования, в которых должна быть возможность установить (как минимум):
  + Интенсивность сканирования
  + Сканирование определённых портов
  + Использование учётной записи
  + Брутфорс учётных записей
  + Выбор уязвимостей для сканирования
* Возможность проведения анализа инфраструктуры на новые уязвимости без необходимости пересканирования инфраструктуры (на основании исторических данных)
* Для безагентного сканирования внутренней корпоративной сети должна использоваться защищённая виртуальная машина(ы)
* Виртуальная машина должна поддерживать все основные платформы виртуализации
* Возможность проверки наличия стандартных паролей на оборудовании
* Возможность аутентификации как минимум на следующих платформах: Windows, Unix, Oracle, Oracle Listener, SNMP, MS SQL, Cisco, IBM DB2, VMware, MySQL, Sybase, Checkpoint Firewall, PostgreSQL, Palo Alto Networks Firewall, MongoDB, HTTP, MS IIS, Apache Web Server, IBM WebSphere App Server, Tomcat Server, Oracle WebLogic Server, Docker
* Возможность интеграции со следующими Password Vaults для получения учётных данных для сканирования: CyberArk PIM Suite, CyberArk AIM, Thycotic Secret Server, Quest Vault, CA Access Control, Hitachi ID PAM, Lieberman ERPM, BeyondTrust PBPS, Hashicorp Vault
* При наличии нескольких систем на одном устройстве (Операционная Система, База Данных, Web сервер и тд) – решение должно позволять оценивать все системы с нужными учётными записями в рамках одного сканирования (автоматически выбирать нужные учётные записи в зависимости от технологий)
* Платформа должна позволять оценивать защищённость инфраструктур, размещённых в публичных облаках: Amazon AWS, Microsoft Azure, Google Cloud Platform
* В Платформе должен быть разделён процесс сканирования от процесса создания отчётов: все сканирования должны наполнять центральную базу по уязвимостям
* Система должна отслеживать статус уязвимости в инфраструктуре и время нахождения в инфраструктуре
* Система должна предоставлять как минимум следующие статусы для уязвимостей в инфраструктуре:
  + новая уязвимость (обнаружена 1 раз)
  + известная уязвимость (обнаружена 2+ раза)
  + исправленная уязвимость (была новой/известной, но система перестала обнаруживать её в инфраструктуре)
  + заново открытая уязвимость (была исправленной, но снова появилась в инфраструктуре)
* Платформа должна позволять обеспечивать непрерывное сканирование критических ресурсов 24/7/365
* Модуль должен позволять добавление своих проверок на уязвимости в формате OVAL или в другом описанном формате. Формат описания сигнатур должен быть задокументирован.

## Требования к отчетности системы анализа защищенности

* Возможность автоматической динамической маркировки устройств на базе предустановленных пользователем правил:
  + По принадлежности к IP подсети
  + На базе парсинга NetBIOS и FQDN имени
  + На базе операционной системы
  + По открытым портам/сервисам
  + По наличию конкретной уязвимости
  + На основании сроков сканирования
* Маркировка должна поддерживать древовидные структуры маркеров с наследованием
* Возможность формирований отчетов как по расписанию, так и по требованию
* Возможность настройки отчётов согласно требованиям компании
* Отчет может / должен содержать следующую информацию:
  + Название уязвимости и уровень ее критичности по шкале вендора и по CVSS
  + Перечень уязвимых систем или сервисов
  + Статус уязвимостей (новая / активная / исправленная)
  + Рекомендации по устранению уязвимости, или ссылку на патч, если таковой существует
  + Дополнительные критерии для приоритезации уязвимости: наличие эксплойта, вредоносного кода, и тд.
* Платформа должна предоставлять возможность фильтрации отчётов по конкретному типу уязвимостей:
  + На базе наличия патча
  + На базе наличия эксплоита в конкретных эксплоит-паках
  + Наличия вредоносного кода для уязвимости
  + CVSS рейтингу (CVSSv2, CVSSv3)
  + Вектору атаки CVSS
  + Вендору и продукту
  + Критичности уязвимости
  + CVE ID
  + И тд.
* Система отчётности должна предоставлять возможность создания тикетов и назначения их на определённых людей
* Возможность формирования отчетов на соответствие стандарту PCI DSS
* Отчеты для руководства. Краткое представление информации с построением графических трендов по результатам сканирования и выявлению или устранению уязвимостей
* Отчёты для IT специалистов по обновлениям, а не по уязвимостям
* Отчёты по успешности прохождения аутентификации при безагентном сканировании систем
* Система должна предоставлять аналитику по обнаруженным уязвимостям и средства для приоритезации устранения уязвимостей
* Система должна в реальном времени показывать статус защищённости ресурсов компании (посредством предустановленных дешбордов)
* Система должна позволять пользователям создавать свои виджеты для дэшбордов
* Система должна обеспечивать возможность выгрузки дэшбордов и виджетов
* Система отчётности должна обеспечивать возможность сквозного поиска по всем проанализированным ресурсам
* Возможность маркировки уязвимости (в случае ложного срабатывания) с последующим исключением из отчётов
* Система должна предоставлять возможность инвентаризации сертификатов с возможностью визуализации информации в виде дэшбордов и поиска по сертификатам, как минимум, должна собираться следующая информация:
  + Certification Authority
  + Алгоритмы шифрования и длина ключа
  + Дата истечения сертификата
* По сертификатам система должна иметь возможность оценивать реализацию HTTPS для веб-серверов
* Система должна предоставлять возможность построения сводных отчётов по инвентаризированным сертификатам как по расписанию, так и по требованию

## Требования к модулю постоянного мониторинга изменений

* Платформа должна позволять обеспечивать непрерывное сканирование на уязвимости критических ресурсов 24/7/365 (в безагнетном и агентском режимах)
* Платформа должна предоставлять пользователям возможность создания правил мониторинга за критичными изменениями, в том числе (но не ограничиваясь):
  + Появлением/изменением устройств в зоне непрерывного сканирования
  + Появлением/устранением уязвимостей на устройствах
  + Открытием/закрытием/изменением портов
  + Установкой/удалением программного обеспечения
  + Появлением/удалением/изменением/истечением сертификатов на сайтах/устройствах
* Платформа должна предоставлять возможность комбинирования условий поиска изменений для создания сложных правил оповещения
* Платформа должна предоставлять возможность оповещения об изменениях только при появлении изменений, оповещение должно происходить по почте сразу после регистрации изменения
* Списки оповещения должны задаваться простым перечислением email адресов

## Требования к модулю приоритезации уязвимостей

* Аналитики вендора, выпускающего платформу, должны отслеживать актуальные атаки на компании по всему миру и предоставлять техническую аналитику по возникающим угрозам
* В аналитических статьях должна описываться сама атака, угроза/ущерб, с помощью каких мер можно предотвратить атаку
* Аналитические статьи, если такое возможно, должны указывать на ранее проанализированные ресурсы Клиента, где обнаружена описанная в статье проблема, которая используется при атаке
* Ко всем уязвимостям, которые может обнаруживать платформа, должны быть добавлены дополнительные аналитические индикаторы, позволяющие дополнительно приоритезировать устранение конкретных уязвимостей. Как минимум должны быть следующие индикаторы:
  + Отсутствие патча для уязвимости
  + Наличие публичного эксплоита
  + Наличие вредоносного кода для уязвимости
  + Лёгкая возможность эксплуатации уязвимости
  + Наличие эксплоита в публичных эксплоит-паках
  + Риск потери данных при эксплуатации уязвимости
  + Риск отказа в обслуживании (DoS) при эксплуатации уязвимости
* Платформа должна иметь предустановленные дэшборды с выведенной информацией по аналитическим индикаторам
* У пользователя Платформы должна существовать возможность использовать аналитические индикаторы в рамках сквозного поиска по инфраструктуре и фильтрации уязвимостей в отчётах
* Платформа должна автоматически калькулировать риски ИБ на основе критичности ИТ-актива и найденных уязвимостей

# Требования к модулю анализа защищенности SSL сертификатов

* Система должна предоставлять возможность производить анализ защищенности сертификатов как с внутренней, так и с внешней инфраструктуры, как минимум, должна предоставляться следующая информация:
  + Имя сертификата
  + Кем выдан (вся цепочка сертификатов)
  + Алгоритмы шифрования и длина ключа
  + Серийный номер и Fingerprint
  + Дата создания и истечения сертификата
  + На каких устройствах используется сертификат
  + Уровень защищенности сертификата
* Должна быть возможность выгрузить сертификат в PEM формате
* Должна быть возможность построения сводных отчётов по инвентаризированным сертификатам как по расписанию, так и по требованию
* Должна быть возможность настраивать автоматические уведомления по почте по заданным правилам
* Система должна предоставлять сквозной поиск по всем сертификатам в инфраструктуре
* Система должна иметь возможность предоставлять информацию о сертификатах в виде динамических дэшбордов

# Требования к модулю управления обновлениями

* Установка обновлений должна осуществляться с помощью агента
* Подсистема должна поддерживать установку системных обновлений на всю, поддерживаемую агентом, линейку ОС Windows, RHEL версий 6, 7, 8, CentOS версий 6, 7, Oracle Linux версий 6, 7, 8, Amazon Linux, и Amazon Linux 2, Ubuntu, Debian
* Подсистема должна поддерживать установку обновлений на прикладное ПО для Windows, как минимум для: Adobe, Google, Mozilla, VMWare, Skype, Oracle, 7-zip, WinSCP и тд
* Вендор должен поддерживать и своевременно обновлять справочники обновлений для ОС/прикладного ПО
* Подсистема должна автоматически отображать список недостающих обновлений на всех IT ресурсах с установленным агентом
* Подсистема должна автоматически отображать уровень критичности обновления, в тех случаях, когда эта критичность задаётся производителем обновления: Low, Moderate, Important, None, Critical
* Подсистема должна позволять фильтровать Superseded обновления (например, кумулятивные обновления, которые перекрывают предыдущие обновления)
* Должна быть возможность гибкой настройки заданий на установку обновлений:
  + Возможность установки обновлений по требованию
  + Возможность установки по расписанию
  + Возможность создания регулярной задачи по обновлению систем с заданной периодичностью (например, задача по ежедневной установке обновлений)
  + Авто-патчинг уязвимостей
  + Авто-патчинг ПО
* Для каждой задачи по установке обновлений должна быть возможность гибко задавать нотификации пользователям, как минимум:
  + Информационное сообщение перед началом процесса обновления
  + Информационное сообщение в процессе обновления
  + Информационное сообщение по завершении процесса обновления
  + Запрос на перезагрузку устройства
  + Сообщение с обратным отсчётом перед перезагрузкой
  + Должна быть возможность отложить перезагрузку (количество раз, которые можно откладывать перезагрузку, должно задаваться)
* В каждую задачу должна быть возможность независимо добавлять:
  + Новые обновления на установку
  + Новые устройства для установки обновлений
* После установки обновления Платформа должна автоматом проверять успешность установки и обновлять данные в Платформе
* Задача на установку обновлений должна понимать, какие обновления применимы к каким устройствам. Задача не должна ставить ненужные обновление на устройства, для которых они не предназначены
* Должен быть механизм сквозного поиска по обновлениям
* Должны быть встроенные дэшборды иллюстрирующие картину установки обновлений в инфраструктуре
* По каждому обновлению должны отображаться уязвимости, которые оно закрывает
* Должна быть возможность создания задач на удаление, установленных ранее обновлений

# Требования к модулю проверки на соответствие требованиям

* Возможность как агентского, так и безагентного сбора информации
* Возможность проведения сканирования на соответствие требованиям как по расписанию, так и по требованию
* Возможность формирований отчетов как по расписанию, так и по требованию
* Графический интерфейс для создания/редактирования политик
* Наличие предустановленных стандартов защищённой конфигурации устройств различных типов, как минимум:
  + CIS
* В любых политиках должна быть возможность редактирования проверок, включённых в политику, и целевых значений
* Должна быть возможность проведение SCAP сканирования и проверки на соответствие SCAP политиками
* Должна быть возможность загрузки собственных SCAP политик
* Возможность проверки одного устройства на соответствие конкретной политике
* Возможность поиска по соответствию всех устройств конкретному требованию
* Должна присутствовать возможность гибкой настройки параметров сканирования
* По результатам оценки инфраструктуры система должна позволять генерировать отчёты, как минимум:
  + Сводный отчёт по соответствию настроек разным политикам безопасности
  + Отчёт по соответствию устройств требованиям конкретной политики безопасности
  + Отчёт по соответствию устройств требованиям конкретной проверки
  + Отчёт по результатам соответствия требований мандатов
* Должна быть возможность создания исключений, с автоматическим отслеживанием статуса исключения
* Открытый API для интеграции с внешними системами