**Приложение № 1 к извещению**

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

# ОБЩИЕ СВЕДЕНИЯ

|  |
| --- |
| Наименование предмета закупки |
| Предоставление неисключительных прав на использование программного обеспечения средство анализа защищенности RedCheck Enterprise или эквивалент (далее – Продукт). |
| ОКПД 2: 26.20.40.146 Системы и средства анализа защищенности, сканеры и анализаторы исходных кодов |
| Состав ПО и иных объектов гражданских прав |
| |  |  |  | | --- | --- | --- | | Наименование | Парт номер / Артикул | Кол-во | | Медиа-комплект для сертифицированной версии Продукта | RC-Media kit | 1 | | Расширение действующей лицензии на использование Продукта в редакции Enterprise на 1 год | RC-EXT-ENT-License-1Y | 1 | |

# ОБЛАСТЬ ПРИМЕНЕНИЯ

|  |
| --- |
| Продукт является средством защиты информации (средством анализа защищенности), реализующим функции автоматизированного обнаружения уязвимостей и контроля конфигураций безопасности (соответствия стандартам и политикам ИБ) в информационных системах неограниченного масштаба с целью оценки возможности преодоления нарушителем системы защиты информационной системы и предотвращения реализации угроз безопасности информации. |

# ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

## Общие требования

* + 1. Лицензионный программный продукт (далее – Продукт) должен обеспечивать функции: обнаружение хостов, сетевой аудит в режиме «Пентест», идентификация открытых сетевых портов и сервисов, подбор паролей к СУБД и сетевым службам, аудиты уязвимостей системного и прикладного программного обеспечения, выявление недостающих обновлений безопасности, аудит конфигурации безопасности согласно указанному профилю, инвентаризацию аппаратного и программного обеспечения сканируемых систем, контроль целостности, аудит уязвимостей платформ контейнеризации аудит уязвимостей АСУ ТП, формирование отчетов по результатам сканирования.
    2. Поставщики Продукта должны предоставить Сертификат соответствия требованиям безопасности информации ФСТЭК России, удостоверяющий соответствие Продукта техническим условиям, средствам контроля (анализа) защищенности информации, Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (ФСТЭК России) – 4 уровень доверия.
    3. Продукт должен реализовать меры защиты ОПС.2, АНЗ.1, АНЗ.2, АНЗ.3, АНЗ.4, ОЦЛ.1, ЗСВ.7 согласно документам «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (утвержден приказом ФСТЭК России № 17 от 11.02.2013) и «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утвержден приказом ФСТЭК России № 21 от 18.02.2013), меры защиты АУД.1, АУД.2, АУД.7, АУД.10, АУД.11, ОЦЛ.1, УКФ.1, ОПО.1, ОПО.2, ОПО.4 согласно документа «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (утвержден Приказом ФСТЭК России № 239 от 25.12.2017г.).
    4. Производитель продукта предоставляет техническую (базовую) поддержку Продукта, включающую:
* Предоставление актуальной документации и других информационных материалов по настройке и эксплуатации Продукта;
* Предоставление новых релизов, обновлений Продукта в соответствии с их лицензионными соглашениями;
* Консультации по порядку доступа и использования «Центра сертифицированных обновлений»;
* Консультация по реализации мер защиты с помощью Продукта.
  + 1. Производитель продукта предоставляет Расширенную техническую поддержку Продукта, включающую:
* Консультации по установке и настройке Продукта в среде Клиента, в том числе и связанные с настройкой среды выполнения;
* Установку и настройку Продукта в среде Клиента посредством сеансов удаленного доступа;
* Рекомендации для достижения оптимального функционирования Продукта в конкретных условиях сети Клиента, в том числе по обеспечению оптимальной производительности и совместимости с используемым Клиентом ПО и техническими средствами;
* Консультации по взаимодействию Продукта с другим ПО и средствами защиты информации;
* Консультации по интерпретации результатов (анализу защищенности) сети Клиента с использованием Продукта;
* Первоочередное предоставление исправлений критических ошибок;
* Консультации по минимизации воздействий ошибок Программы (в случае их подтверждения специалистами Производителя) до выхода очередного исправления;
* Модификация включенных в Продукт конфигураций безопасности под условия применения (среду) Клиента.
  + 1. Сроки поставки Продукта – в течение 15 (пятнадцати) рабочих дней с даты заключения договора.

## Требования к основным параметрам и характеристикам

* + 1. Продукт должен функционировать под управлением операционных систем:
* Astra Linux Special Edition 1.7;
* Debian 12;
* РЕД ОС 7.3;
* Microsoft Windows Server 2019 / 2022.
  + 1. Управление Продуктом должно осуществляться с помощью единой веб-консоли, доступной в сети ИТ-инфраструктуры, с использованием стандартизованного веб-браузера. Опубликованная веб-консоль должна быть защищена с помощью SSL-сертификата, выданного внутренним центром сертификации ИТ-инфраструктуры.
    2. Лицензия на Продукт должна иметь ограничение на не менее 500 одновременно добавленных в Продукт элементов ИТ-инфраструктуры, для возможности сканирования, просмотра результатов и контроля. Пользователь должен иметь возможность в пределах имеющейся у него лицензии изменять, добавлять, удалять сканируемые элементы ИТ-инфраструктуры (IP-адреса, FQDN) без изменения, имеющегося у него лицензионного ключа.
    3. Продукт должен реализовывать хранение решающих правил (сигнатур), сканируемых объектов ИТ-инфраструктуры, настроек подключения и Продукта с использованием системы управления реляционными базами данных Microsoft SQL Server, PostgreSQL Server, Jatoba, Pangolin.
    4. Продукт должен реализовывать возможность подключения и раздельного использования дополнительных модулей сканирования, обеспечивающих размещение на выделенных площадках (геораспределенность), распределение нагрузки, разграничение заданий сканирования и возможность масштабирования Продукта.
    5. Продукт должен реализовывать обновление базы решающих правил (сигнатур):
* с использованием репозитория обновлений базы решающих правил Производителя в сети Интернет, защищенных SSL-сертификатом;
* с использованием репозитория обновлений базы данных решающих правил Производителя в сети Интернет, защищенных SSL-сертификатом, с помощью прокси-сервера в сети ИТ-инфраструктуры;
* с использованием локального адреса (директории), после загрузки обновлений базы данных решающих правил с сайта Производителя, защищенного парой логин-пароль.
  + 1. Продукт должен реализовывать определение перечня сканируемых узлов на основе ключевого атрибута – FQDN (полное доменное имя), IP-адрес элемента ИТ-инфраструктуры:

1. вводом данных о сканируемых узлах в ручном режиме на основании ключевого атрибута;
2. интеграцией с единым каталогом домена Microsoft Active Directory для импорта списка узлов из базы данных домена элементов ИТ-инфраструктуры;
3. импортом данных из CSV-файла, содержащем ключевые атрибуты.
4. импортом результатов с обнаруженными узлами сети с помощью сетевого сканирования.
   * 1. Продукт должен иметь в рамках отдельного задания, выполнения его по расписанию и создания отчета возможность обнаружения узлов сети по заданному диапазону, импорта их в систему, возможность экспорта во внешний файл в формате CSV, содержащего информацию по обнаруженным активам в рамках сетевого сканирования.
     2. Результаты сетевого аудита «Обнаружение хостов» в рамках обнаружения узлов сети должны отображаться в графическом окне Продукта и содержать:
5. Количество обнаруженных узлов сети;
6. Количество новых узлов сети в сравнении с ранее добавленными;
7. Способ обнаружения;
8. IP-адрес;
9. DNS;
10. FQDN;
11. NetBIOS;
12. Данные об установленной операционной системе в виде CPE;
13. Информацию о наличии доступного агента Продукта.
    * 1. Продукт должен реализовывать аудит в режиме «Пентест» в рамках сетевого сканирования:
14. Продукт должен обеспечивать сканирование портов заданной группы сетевых узлов с возможностью выбора режима профиля, диапазона и типов портов TCP или UDP, с результатом идентификации открытых портов и сервисов в графическом окне Продукта;
15. Продукт должен обеспечивать поиск уязвимостей с возможностью выбора точности сканирования;
16. Продукт должен обеспечивать возможность создания и сохранения для дальнейшего использования собственного профиля сканирования;
17. Продукт должен обеспечивать подбор паролей в виде пары «логин-пароль» для локальных учетных данных к опубликованным сетевым службам Microsoft SQL, PostgreSQL, OracleDB, MySQL, SSH, FTP, POP3 методом полного перебора с возможностью использования внешних словарей, результаты которого должны отображаться в графическом окне Продукта;
18. Продукт должен иметь встроенную базу «логин-пароль», содержащую не менее 5000 записей, а также иметь возможность подключения собственных словарей.
19. Продукт должен обеспечивать возможность обнаружения уязвимостей в Java-архивах для Unix-систем с возможностью указания пользовательских путей хранения.
    * 1. Результаты сетевого аудита в режиме «Пентест» в рамках поиска уязвимостей должны отображаться в графическом окне Продукта и содержать:
20. идентификатор уязвимости ALTXID, BDU ID, CVE (при наличии);
21. сетевой порт, на котором обнаружена уязвимость;
22. уровень риска обнаруженной уязвимости;
23. уровень точности, используемый при сканировании.
24. описание уязвимости;
25. продукты, в которых обнаружена уязвимость;
26. определение применимости уязвимости CPE;
27. векторы уязвимости CWE, CVSSv2, CVSSv3;
28. детализация программного обеспечения обнаруженной уязвимости;
    * 1. Продукт должен реализовывать системный аудит уязвимостей системного и прикладного программного обеспечения:
29. Продукт должен обеспечивать сигнатурный анализ данных, собранных при системном сканировании сетевого узла и предоставлять информацию об обнаруженных уязвимостях;
30. Продукт должен обеспечивать сканирование группы сетевых узлов;
31. Продукт должен обеспечивать возможность множественного выбора учетных данных для аутентификации на узлах;
32. Продукт должен обеспечивать возможность повторного сканирования недоступных сетевых узлов в рамках одной задачи;
33. Продукт должен обеспечивать сканирование следующих платформ:

* Microsoft Windows:
  + Microsoft Windows Server 2003 / 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 / 2019 / 2022;
  + Microsoft Windows XP SP3 / Vista / 7 / 8 / 8.1 / 10 / 11;
* Linux:
  + CentOS Linux 5 / 6 / 7/ 8;
  + CentOS Stream 8 / 9;
  + Debian 6 / 7 / 8 / 9 / 10 / 11 / 12;
  + Debian GNU / kFreeBSD 6 / 7;
  + Debian GNU / Linux 2.2 /3.0 /3.1 / 4 / 5 / 6 / 7;
  + Red Hat Enterprise Linux 5 / 6 / 7 / 8 / 9;
  + Ubuntu 4.10 / 5.04 / 5.10 / 6.06 / 6.10 / 7.04 / 7.10 / 8.04 / 8.10 / 9.04 / 9.10 / 10.04 /10.10 / 11.04 / 11.10 / 12.04 / 12.10 / 13.04 / 13.10 / 14.04 / 14.10 / 15.04 / 15.10 / 16.04 / 16.10 / 17.04 / 17.10 / 18.04 / 20.04 / 22.04 / 22.10 / 23.04 / 23.10;
* Российские ОС:
  + Ред ОС Муром 7.1 / 7.2 / 7.3;
  + ALT Linux 6 / 7;
  + ALT Linux SPT 6 / 7;
  + ALT 8 SP / 10 SP;
  + ALT 9 / 10;
  + Astra Linux SE Орел/Воронеж/Смоленск 1.5 / 1.6 / 1.7;
  + Astra Linux CE Орел 2.12;
* Сетевое оборудование:
  + CheckPoint GAiA;
  + Cisco IOS;
  + Cisco NX-OS;
  + Huawei VRP;
  + Eltex;
  + FortiGate FortiOS 5.0;
  + UserGate UTM 6.1.5.11134R;
  + UserGate UTM 6.1.0.10123F;
* Виртуализация:
  + Microsoft Hyper-V Server 2008 / 2008 R2 / 2012 / 2012 R2;
  + VMware ESXi Server 5.1 / 5.5 /6.0 / 6.5 / 6.7 / 7;
  + VMware vCenter Server 5.1 / 5.5 / 6.0 / 6.7 / 7;
  + VMware NSX
  + VMware Photon OS 1.0 / 2.0 / 3.0 / 4.0;
* СУБД:
  + Microsoft SQL Server 2005 / 2008 / 2008 R2 / 2012 / 2014 / 2016 / 2017 / 2019 / 2022;
  + MySQL Server 4.1 / 5.0 / 5.1 / 5.5 / 5.6 / 5.7 / 6.0 / 8.0 / 8.1 / 8.2;
  + Oracle Database Server 11 / 12 / 18 / 19;
  + PostgreSQL 8 / 9 / 10 / 11 / 12 / 13 / 14 / 15 / 16;
* Офисные пакеты:
  + LibreOffice;
  + Microsoft Office;
  + R7-Office;
* Контейнеризация:
  + Docker 1.13.0 (Storage Driver overlay2);
  + Kubernetes 1.18 / 1.19 / 1.20 / 1.21 / 1.22 / 1.23 / 1.24.
    1. Результаты аудита уязвимостей должны отображаться в графическом окне Продукта и содержать:

1. название уязвимости;
2. идентификатор уязвимости в БД УБИ <BDU ID> (ФСТЭК России);
3. идентификатор уязвимости CVE;
4. векторы уязвимости CVSSv2, CVSSv3, CWE;
5. уровень опасности обнаруженной уязвимости;
6. описание уязвимости;
7. рекомендуемые меры по устранению уязвимости;
8. наименование ПО, подверженного уязвимости;
9. детализация пути расположения уязвимого ПО;
10. ссылки на БДУ УБИ и ресурсы-источники, в которых содержатся сведения об обнаруженных уязвимостях.
    * 1. Продукт должен реализовывать системный аудит уязвимостей образов контейнеризации Docker с возможностью множественного выбора учетных данных для авторизации, а также возможностью повторного сканирования недоступных сетевых узлов с указанием количества и интервалов попыток в рамках одной задачи, результаты которой должны отображаться в графическом окне Продукта и для каждого узла содержать:
11. количество образов;
12. количество уязвимых образов;
13. количество образов с уязвимостями высокого риска;
14. наименование репозитория образа;
15. количество уязвимостей для образа;
16. количество контейнеров на основе образа;
17. теги образа;
18. размер образа;
19. операционная система образа;
20. архитектура образа;
21. дата создания образа;
22. уникальное имя образа (хэш).
    * 1. Продукт должен реализовывать системный аудит обновлений безопасности с возможностью множественного выбора учетных данных для авторизации, а также возможностью повторного сканирования недоступных сетевых узлов с указанием количества и интервалов попыток в рамках одной задачи, результаты которой должны отображаться в графическом окне Продукта и для каждого узла содержать:
23. наименование обновления;
24. сведения о рисках, связанных с отсутствием недостающего обновления на узле;
25. ссылку на производителя, заявившего о выходе обновления;
26. ссылку на доступное для загрузки обновление в репозитории производителя или аналогичном доверенном хранилище.
    * 1. Продукт должен реализовывать системный аудит конфигураций безопасности с возможностью множественного выбора учетных данных для авторизации, а также возможностью повторного сканирования недоступных сетевых узлов с указанием количества и интервалов попыток в рамках одной задачи, выполнять проверку соответствия настроек параметров безопасности системного и прикладного ПО, включая СУБД и платформы контейнеризации, по заданному конфигурационному профилю. Результаты аудита должны отображаться в графическом окне Продукта и содержать информацию о степени соответствия сканируемого узла выбранному профилю безопасности:

* Microsoft Windows Server 2003 / 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 / 2019 / 2022 (включая роли серверов);
* Microsoft Windows XP SP3 / 7 / 8 / 8.1 / 10 / 11;
* Astra Linux Special Edition / Смоленск / Орел;
* ALT 8 / 9 / 10;
* CentOS Linux 5 / 6 / 7 / 8;
* Debian 6 / 7 / 8 / 9 / 10 / 11 / 12;
* Red Hat Enterprise Linux 5 / 6 / 7 / 8 / 9;
* Ubuntu 12.04 / 13.10 / 14.04 / 14.10 / 15.04 / 15.10 / 16.04 / 16.10 / 17.04 / 17.10 / 18.04 / 18.10 / 19.04 / 19.10 / 20.04 / 20.10 / 21.04 / 21.10 / 22.04 / 22.10 / 23.04 / 23.10 / 24.04;
* Cisco IOS;
* Cisco NX-OS;
* Huawei VRP;
* CheckPoint GAiA;
* UserGate Unified Threat Management (UTM) 6 / 7;
* VMware vCenter 5 / 6;
* VMware ESXi 5 / 6 / 7 / 8;
* VMware NSX;
* Docker;
* Kubernetes;
* Microsoft SQL Server 2005 / 2008 / 2008 R2 / 2012 / 2014 / 2016 / 2017 / 2019;
* MySQL Server 5.5 / 5.6 / 5.7 / 8.0;
* Oracle Database Server 11 / 12 / 18 / 19;
* PostgreSQL 8 / 9 / 10 / 11 / 12 / 13 / 14 / 15 / 16;
* Apache HTTP Server;
* Apache Tomcat 6 / 7 / 8;
* Веб-сервер Nginx;
* Компонент PHP;
* Microsoft IIS и .Net;
* Microsoft Office / 2013 / 2016 / 2019 / 365;
* Стандарт PCI DSS 3.2.1;
* Конфигурация ГИС. Класс 3 / 4;
* Средства защиты информации КриптоПРО CSP, Континент-АП, AppLocker, SRP.
  + 1. Продукт должен обладать инструментами по модификации состава и значений параметров профилей аудита и создания собственных конфигураций на основе существующих.
    2. Продукт должен реализовывать фиксацию и контроль целостности каталогов и файлов по выбранной маске наименования методом контрольного суммирования MD5, SHA1, SHA256, SHA512, ГОСТ Р 34.11-2012.
    3. Продукт должен реализовывать инвентаризацию программного и аппаратного обеспечения с возможностью множественного выбора учетных данных для авторизации, а также возможностью повторного сканирования недоступных сетевых узлов с указанием количества и интервалов попыток в рамках одной задачи, результаты которой должны отображаться в графическом окне Продукта и для каждого узла содержать:

1. для сканируемых узлов с операционной системой Microsoft Windows:

Аппаратное обеспечение:

* + Список CPU;
  + Материнская плата;
  + BIOS;
  + Слоты памяти;
  + Видеоконтроллеры;
  + Сетевые адаптеры;
  + Физические диски;
  + Логические диски;
  + Приводы чтения лазерных дисков;
  + USB – устройства.

Программное обеспечение:

* + Информация об операционной системе;
    - Имя;
    - Версия;
    - Пакет обновлений;
    - Производитель;
    - Архитектура;
    - Тип продукта;
    - Уровень шифрования;
    - Системный каталог;
    - Системный диск;
    - Код страны;
    - Версия IE;
    - Организация;
    - Дата установки;
    - Входит в домен;
    - Домен/рабочая группа;
    - Роль в домене;
    - Переменные среды;
    - Локальные группы;
    - Локальные пользователи;
    - Службы;
    - Общие папки;
    - Обновления для системы безопасности;
    - Накопительные пакеты обновлений;
    - Исправления;
    - Пакеты обновлений;
    - Обновления;
    - Обновления QFE.
  + Установленное ПО;
  + Дополнительные компоненты;
  + Компоненты сервера.

OVAL-инвентаризация.

1. для сканируемых узлов с операционной системой семейства Linux:

Аппаратное обеспечение:

* + Список CPU;
  + Материнская плата;
  + BIOS;
  + Слоты памяти;

Программное обеспечение:

* + Информация об операционной системе;
    - Имя;
    - Версия;
    - ID;
    - Имя хоста;
    - Платформа;
    - Ядро;
    - LSB-релиз;
    - Systemd релиз;
    - Сетевые интерфейсы;
    - DNS-сервера;
    - ARP-таблица;
    - Таблица маршрутизации;
    - Сетевой резолвер;
    - Переменные среды;
    - Локальные пользователи;
    - Локальные группы;
  + Информация об установленных пакетах;
  + Информация о контейнерах;

OVAL-инвентаризация.

1. для сканируемых узлов с платформой VMware ESXi Server:

Хосты:

* Имя хоста;
* Полное имя;
* Версия;
* Сборка;
* Тип ОС;
* UUID;
* Тип API;
* Версия API;

Аппаратное обеспечение:

* + Материнская плата;
  + BIOS;
  + Список CPU;
  + Слоты памяти;
  + Видеоконтроллеры;
  + Сетевые адаптеры;
  + Хранилища данных.

Программное обеспечение:

* + Локальные группы;
  + Локальные пользователи;
  + Image Profile;
  + Lockdown Mode;
  + Пользователи Lockdown Mode;
  + Наборы правил брандмауэра;
  + Службы;
  + Пакеты;
  + Настройки.

OVAL-инвентаризация.

1. для сканируемых узлов с платформой VMware vCenter Server:

Виртуальный центр:

* Имя хоста;
* Полное имя;
* Версия;
* Сборка;
* Тип ОС;
* UUID;
* Тип API;
* Версия API.

Программное обеспечение.

Хосты:

* Имя хоста;
* Полное имя;
* Версия;
* Сборка;
* Тип ОС;
* UUID;
* Тип API;
* Версия API;

Аппаратное обеспечение:

* + - * + Материнская плата;
        + BIOS;
        + Список CPU;
        + Слоты памяти;
        + Видеоконтроллеры;
        + Сетевые адаптеры;
        + Хранилища данных.

Программное обеспечение:

* + Локальные группы;
  + Локальные пользователи;
  + Image Profile;
  + Lockdown Mode;
  + Пользователи Lockdown Mode;
  + Наборы правил брандмауэра;
  + Службы;
  + Пакеты;
  + Настройки.

Виртуальные машины:

* Имя;
* Имя гостя;
* Состояние гостя;
* UUID.

Аппаратное обеспечение:

* Количество процессоров;
* Количество ядер;
* Слоты памяти;
* Физические диски;
* Сетевые адаптеры;
* Видеоконтроллеры;
* Оптические приводы;
* Накопители на гибких дисках.

Программное обеспечение:

* Настройки.

OVAL-инвентаризация.

1. для сканируемых узлов с платформой VMware NSX Server:

Аппаратное обеспечение:

* Список CPU;
* Объем оперативной памяти;
* Объем хранилища данных.

Программное обеспечение:

* Операционная система;
* Сетевые параметры;
* Single Sign-On (SSO);
* vCenter Server;
* Безопасность;
* Пользователи;
* Службы.

OVAL-инвентаризация.

1. для сканируемых узлов с платформой Cisco IOS:

Аппаратное обеспечение:

* + Модель;
  + Список CPU;
  + Количество оперативной памяти;
  + Устройство хранения данных и объем
  + Серийный номер шасси;
  + Серийный номер материнской платы;
  + Серийный номер блока питания.

Программное обеспечение:

* + Версия Cisco IOS;
  + Семейство;
  + Имя узла;
  + Домен узла;
  + Значение конфигурационного регистра;
  + Файловая система;
  + Конфигурационные файлы;
  + Службы;
  + Локальный пользователи;
  + Списки доступа;
  + ARP-таблица;
  + Терминальные линии;
  + SNMP-строки;
  + Служба регистрации событий
  + Сетевые интерфейсы, включая Mac-адрес, IP-адреса и списки доступа;

OVAL-инвентаризация.

1. для сканируемых узлов с платформой Cisco NX-OS:

Аппаратное обеспечение:

* Список CPU;
* Количество оперативной памяти;
* Серийный номер шасси;
* Аппаратные сменные модули (FRU).

Программное обеспечение:

* Версия NX-OS;
* Семейство;
* Имя узла;
* Домен узла;
* Конфигурационные файлы;
* Службы;
* Локальный пользователи;
* Списки доступа;
* Терминальные линии;
* SNMP-строки;
* Сетевые интерфейсы, включая Mac-адрес, IP-адреса и списки доступа.

OVAL-инвентаризация.

1. для сканируемых узлов с платформой UserGate:

Программное обеспечение:

* + Версия ОС;
  + GUID;
  + Имя хоста;
  + Сетевые интерфейсы;
  + Администраторы;
  + Профили;
  + Парольная политика.

OVAL-инвентаризация.

1. для сканируемых узлов с платформой CheckPoint GAiA:

Аппаратное обеспечение:

* + Устройство;
  + Платформа;
  + Модель;
  + Серийный номер;
  + Список CPU;
  + Объем оперативной памяти;
  + Физический накопитель и объем;
  + Сетевые адаптеры.

Программное обеспечение:

* + Версия GAiA;
  + Параметры сетевых интерфейсов;
  + Перечень исправлений;
  + Перечень продуктов с исправлениями.

OVAL-инвентаризация.

* + 1. Продукт должен реализовывать установку выполненных заданий аудита уязвимостей, аудита конфигураций, инвентаризации и фиксации на контроль для дальнейшего их сравнения с контролируемыми текущими значениями. Результаты должны отображаться в графическом окне Продукта и содержать:
* Номер контроля;
* Ключевой атрибут сетевого узла;
* Статус контроля;
* Наименование задания сканирования;
* Номер задания сканирования;
* Тип задания сканирования;
* Дата создания контроля;
* Дата завершения задания сканирования;
* Детализация соответствия контроля в части добавления, удаления и изменения контролируемых объектов.
  + 1. Продукт должен обеспечивать создание заданий по сканированию узлов с параметрами, определяющими время запуска:
* выполнение задания сканирования сразу после создания;
* определение максимального времени работы задания сканирования;
* повторное сканирование неуспешных узлов сети в рамках одной задачи;
* разовое выполнение задания сканирования в назначенное время;
* выполнение задания сканирования по расписанию с заданной периодичностью.
  + 1. Продукт должен иметь в рамках отдельного задания, выполнения его по расписанию и создания отчета возможность проверки сетевого туннеля в агентном и безагентном режимах системного сканирования, с возможностью множественного выбора привилегированных учетных записей и соответствующих стандартизованных протоколов SSH, HTTP, WinRM c использованием протокола Kerberos.
    2. Продукт должен обеспечивать возможность выявления актуальности сканирования и причин недоступности узлов или групп узлов за указанный период времени. Результат должен быть доступен в интерфейсе в виде таблицы и иметь возможность экспорта в CSV-отчет, включая данные:

1. Наименование узла IP / DNS;
2. Причину отсутствия актуальных результатов сканирования;
3. Принадлежность или отсутствие принадлежности узла к группе.
   * 1. Продукт должен обеспечивать возможность выявления детализированной причины недоступности узла или групп узлов за указанный период времени. Результат должен быть доступен в интерфейсе в виде таблицы и иметь возможность экспорта в CSV-отчет, включая данные:
4. Наименование узла IP / DNS;
5. Тип сканирования задания;
6. Наименование задания;
7. Результат сканирования;
8. Причина недоступности узла;
9. Завершение сканирования.
   * 1. Продукт должен обеспечивать возможность проводить анализ сетевой инфраструктуры на предмет наличия уязвимостей на узлах или группах узлов за выбранный период времени или при помощи выбора определенного задания сканирования с использованием встроенного фильтра:

Встроенный фильтр обеспечивает возможность выбора:

1. Задания сканирования;
2. Выбранного периода в днях;
3. Уровня критичности для уязвимостей;
4. Уровня оценки уязвимости по стандарту CVSSv2 и CVSSv3;
5. Уязвимостей с наличием эксплойта;
6. Банков данных уязвимостей;
7. Дату публикации бюллетеня безопасности вендором.

Результат должен обеспечивать возможность получения информации с помощью вкладок, быть доступен в интерфейсе в виде таблицы и иметь возможность экспорта в CSV-отчет, включая данные:

1. Уязвимости:

* Внутренний идентификатор уязвимости ALTX ID;
* Уровень риска уязвимости;
* Уровень оценки уязвимости CVSS;
* Наименование уязвимости;
* Дата публикации уязвимости;
* Количество узлов, подверженных уязвимости;
* Список узлов, подверженные уязвимости.

1. «Хосты»:

* Наименование узла IP / DNS;
* Всего уязвимостей на узлах;
* Уровень риска выявленных уязвимостей;
* Перечень уязвимостей на выбранном узле.

1. «Хост – уязвимость»:

* Наименование узла IP / DNS;
* Внутренний идентификатор уязвимости ALTXID;
* Уровень риска уязвимости;
* Уровень оценки уязвимости;
* Наименование уязвимости;
* Дата публикации уязвимости.
  + 1. Продукт должен обеспечивать возможность проводить сравнение состояния сетевой инфраструктуры на предмет наличия уязвимостей на узле или на группе узлов с возможностью выбора задания сканирования, а также выбора временного интервала между двумя успешными сканированиями с использованием встроенного фильтра.

Встроенный фильтр обеспечивает возможность выбора:

1. Задания сканирования;
2. Завершенных успешных сканирований;
3. Выбранного периода в днях;
4. Уровня критичности для уязвимостей;
5. Уровня оценки уязвимости по стандарту CVSSv2 и CVSSv3;
6. Уязвимостей с наличием эксплойта;
7. Банков данных уязвимостей;
8. Дату публикации бюллетеня безопасности вендором.

Результат должен обеспечивать возможность получения информации с помощью вкладок, быть доступен в интерфейсе в виде таблицы и иметь возможность экспорта в CSV-отчет, включая данные:

1. Уязвимости:

* Внутренний идентификатор уязвимости ALTXID;
* Уровень риска уязвимости;
* Уровень оценки уязвимости CVSS;
* Наименование уязвимости;
* Дата публикации уязвимости;
* Новая уязвимость для узлов;
* Неустраненная уязвимость для узлов;
* Устраненная уязвимость для узлов;
* Перечень узлов.

1. Хосты:

* Наименование узла IP / DNS;
* Новые уязвимости на узле;
* Уязвимости с критическим и высоким уровнем риска на узле;
* Количество неустраненных уязвимостей для узла;
* Количество неустраненных уязвимостей с критическим и высоким уровнем риска на узле;
* Количество устраненных уязвимостей на узле;
* Количество устраненных уязвимостей с критическим и высоким уровнем риска на узле;
* Список уязвимостей.

1. Хост – уязвимость:

* Наименование узла IP / DNS;
* Внутренний идентификатор уязвимости ALTXID;
* Статус устранения уязвимости на узле;
* Уровень риска уязвимости;
* Наименование уязвимости;
* Дата публикации уязвимости.
  + 1. Продукт должен обеспечивать возможность проверки узла или группы узлов в процентном соотношении на соответствие конфигурациям безопасности, выполнять проверку соответствия настроек параметров безопасности системного и прикладного ПО, включая СУБД и платформы контейнеризации по заданному конфигурационному профилю с возможностью выбора задания сканирования, а также выбора временного интервала.

Результат должен обеспечивать возможность получения информации с помощью вкладок, быть доступен в интерфейсе в виде таблицы, включая данные:

1. Статистика:

* Наименование конфигурации безопасности и количество правил;
* Профиль конфигурации безопасности и количество правил;
* Результаты сканирования узлов;
* Диаграмма уровня соответствия узлов для проверяемой конфигурации безопасности.

1. Правила:

* Порядковый номер проверяемого правила;
* Наименование проверяемого правила;
* Уровень риска проверяемого правила;
* Количество узлов, соответствующие проверяемому правилу;
* Количество узлов, несоответствующих проверяемому правилу;
* Количество узлов в статусе «Ошибка» или «Неизвестно»;
* Количество узлов, к которым неприменимо проверяемое правило.

1. Хосты:

* Наименование узла IP / DNS;
* Процент соответствия конфигурации безопасности;
* Статус соответствия конфигурации безопасности;
* Количество соответствующих правил для узла;
* Количество несоответствующих правил для узла;
* Уровень риска несоответствующих правил для узла;
* Количество неизвестных правил для узла;
* Количество ошибочных правил для узла;
* Количество неприменимых правил для узла.

1. Хост – параметр:

* Наименование узла IP / DNS;
* Результат соответствия выбранного правила;
* Фактический параметр.
  + 1. Продукт должен реализовывать формирование отчетов по предварительно заданному профилю сканирования с возможностью определять количественные оценки уязвимостей в безопасности компьютерной системы по стандартам CVSSv2 и CVSSv3 по результатам сканирования в форматах HTML, PDF, MHT, CSV, XML:
* отчет по выбранному диапазону элементов ИТ-инфраструктуры, по последним результатам сканирования;
* отчет по выбранному заданию сканирования;
* дифференциальный отчет, сравнивающий два результата сканирования одной задачи за разные промежутки времени.
  + 1. Сформированный отчет по результатам сканирования должен содержать следующие разделы:
* статистические данные аудита в виде диаграммы или таблицы;
* сводную информацию о результатах аудита;
* детализированную информацию о данных аудита, сгруппированную по сканируемым элементам ИТ-инфраструктуры.
  + 1. Сформированный отчет по результатам аудита конфигураций безопасности должен содержать:
* иерархию проверяемых параметров, сгруппированных по классификационному признаку;
* сводные данные по количеству параметров с различными состояниями (соответствует эталонному значению/ не соответствует эталонному значению/ не проверено);
* ссылку на классификатор CCE;
* описание настройки проверяемого параметра;
* эталонное (рекомендованное) значение параметра;
* текущее значение проверяемого параметра;
* описание варианта конфигурации параметра для соответствия рекомендованным значениям.
  + 1. Продукт должен обеспечивать возможность формирования отчетов по заранее созданному шаблону и отправку отчетов по результатам сканирования заданному списку получателей на электронный почтовый ящик, сетевой каталог.
    2. Продукт должен обеспечивать удаление неактуальных результатов сканирований и отчётов для уменьшения размера баз данных вручную и по заданному расписанию, а также уведомлять о превышении размеров баз данных на указанный адрес электронной почты.
    3. Продукт должен обеспечивать контроль целостности собственных исполняемых файлов, отвечающих за реализацию механизмов безопасности, с использованием метода контрольного суммирования.
    4. Продукт должен иметь возможность диагностики собственных служб в графическом окне Продукта, включая проверку работоспособности базы данных, службы синхронизации, службы сканирования и состояния лицензии на Продукт.
    5. Продукт должен иметь возможность мониторинга дополнительных модулей сканирования, размещенных на выделенных площадках. Информация о дополнительных модулях сканирования должна отображаться в интерфейсе программы и содержать информацию:

1. Порядковый номер дополнительного модуля сканирования;
2. Индикатор доступности дополнительного модуля сканирования;
3. Наименование дополнительного модуля сканирования;
4. Среда функционирования дополнительного модуля сканирования;
5. Дату и время последнего обращения к базе данных.
   * 1. Производитель Продукта должен предоставить доступ к описаниям уязвимостей, хранящимся на специализированном портале, доступном в сети Интернет:
6. На специализированном портале Производителя должны содержаться описания уязвимостей и ссылки на источники информации, базы знаний;
7. Описания баз уязвимостей, используемых Продуктом, должны быть выполнены в соответствии с требованиями:

* ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем»;
* ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей»;

1. В качества языка описания уязвимостей должен использоваться стандартизованный язык OVAL;
2. Классификаторы уязвимостей, перечни идентифицируемых продуктов, степень опасности, критерии опасности и другая информация о выявленных проблемах безопасности должны быть стандартизованы и выполнены с поддержкой протокола SCAP (Security Content Automation Protocol).
   * 1. Продукт должен иметь возможность импорта и использования сторонних OVAL-определений, предоставляемых Производителем продукта или другими авторитетными источниками.
     2. Продукт должен обеспечивать возможность аутентификации в единой Web-консоли управления с помощью внутренних локальных учетных записей, а также с помощью Windows-аутентификации с использованием протокола Kerberos.
     3. Продукт должен поддерживать дополнительный механизм защиты системы с использованием технологии визуально-графического подтверждения ввода символов CAPTCHA.
     4. Продукт должен обеспечивать разграничение прав доступа пользователей на основе групп безопасности:

* Администратор Продукта с полными правами;
* Администратор безопасности;
* Пользователь Продукта;
* Администратор обслуживания Продукта, для выполнения обновлений, обслуживания учетных записей сканирования и сканируемых сетевых узлов, диагностики и устранения проблем.

# ТРЕБОВАНИЯ К УСЛОВИЯМ ПОСТАВКИ

|  |
| --- |
| Продукт передается в составе:   * лицензия(и) правообладателя на бумажном носителе с указанием количества сканируемых IP-адресов и срока действия лицензии; * Медиа-комплект (не менее одного комплекта на поставку), содержащий:   + верифицированный дистрибутив с программой на USB-носителе;   + руководства по установке, настройке и работе с Продуктом;   + формуляр на сертифицированный Продукт, промаркированный голографическим знаком соответствия ФСТЭК России;   + копия сертификата ФСТЭК России на сертифицированный Продукт, заверенный производителем;   + сертификат на расширенную техническую поддержку (при необходимости). |

# ТРЕБОВАНИЯ К ОБЪЕМУ И СРОКУ ПРЕДОСТАВЛЕНИЯ ГАРАНТИЙ

|  |
| --- |
| * 1. Срок, на который предоставляются права на Продукт – 12 (двенадцать) месяцев с момента передачи Заказчику неисключительных прав на программное обеспечение в период с 15.05.2025 по 14.05.2026.   2. Поставщик передает Заказчику Лицензии правообладателя на бумажном носителе. Ключи активации передаются правообладателю в бумажном и электронном виде;   3. Срок расширенной технической поддержки – 12 (двенадцать) месяцев с момента активации лицензии (при необходимости). |

# ТРЕБОВАНИЯ ПО БЕЗОПАСНОСТИ

|  |
| --- |
| Продукт не должен содержать вирусов, троянских программ и каких-либо программ, исполняемых не по прямому назначению данного программного обеспечения. |

# ТРЕБОВАНИЯ К КАЧЕСТВУ И СЕРТИФИКАЦИИ

|  |
| --- |
| Продукт должен быть включен в Единый реестр российских программ для электронных вычислительных машин и баз данных, введенный в действие в соответствии с Постановлением Правительства Российской Федерации от 16.11.2015 № 1236.  Продукт должен иметь действующий сертификат ФСТЭК России для средств контроля (анализа) защищенности информации. |