### Функциональные требования

#### В ходе проведения работ должна быть внедрена система комплексного решения для анализа защищенности и управления ИБ предприятий “Redcheck”. Используемые функциональные возможности продукта должны быть определены в ходе технического проектирования. Работы по проектированию выполняются Исполнителем. В ходе проведения работ Исполнитель оставляет за собой право выдачи рекомендаций для обеспечения соответствия выполнения мер безопасности Приказов ФСТЭК 17 и 21.

#### Продукт должен обеспечивать выполнение функций обнаружения хостов, аудитам в режиме (“Пентест”, уязвимостей, конфигураций, СУБД, АСУ ТП, систем контейнеризации), инвентаризации, фиксации, проверке доступности и документированию результатов аудита (Отчеты) на следующих системах:

#### Windows…

#### Продукт должен осуществлять:

1. Обнаружение хостов
2. Аудит в режиме «Пентест»
3. Аудит уязвимостей
4. Аудит обновлений
5. Аудит конфигураций
6. Инвентаризация
7. Фиксация (контроль целостности)
8. Аудит СУБД
9. Аудит систем контейнеризации
10. Аудит уязвимостей АСУ ТП
11. Проверка доступности
12. Документирование результатов аудита (Отчеты)
13. Функция Контроль

#### Продукт применяется для решения следующих задач:

#### централизованное сетевое или локальное определение уязвимостей системного и прикладного ПО, аппаратных платформ;

#### контроль настроек параметров безопасности, соблюдения требований политик и стандартов ИБ;

#### инвентаризация оборудования и ПО;

#### контроль целостности файлов и каталогов;

#### создание отчетов по результатам аудитов.

#### выявление и идентификацию информационных ресурсов, перечисленных в п.п. 4.4.1.1 настоящего ТЗ и функционирующих в момент сканирования;

#### сбор идентификационных данных об информационных ресурсах (IP-адрес, hostname/FQDN);

#### выявление и идентификацию доступных в момент сканирования портов, использующих сетевые протоколы транспортного уровня;

* сбор следующих сведений об информационных ресурсах по протоколам удаленного управления: WMI, SSH, Telnet, ODBC, SNMP, Checkpoint OPSEC:
* для ОС семейства Windows:
* информация о сетевой конфигурации,
* информация об аппаратных компонентах,
* информация об установленном программном обеспечении (наименование, версия, путь установки),
* перечень процессов и служб, обнаруженных при сканировании;
* для ОС семейства Unix\Linux:
* информация о сетевой конфигурации,
* информация об аппаратных компонентах,
* информация об установленных пакетах,
* информация о сервисах и службах, обнаруженных при сканировании;
* для активного сетевого оборудования:
* информация о сетевых интерфейсах,
* информация о пользователях,
* информация о списках контроля доступа;
* для СУБД:
* пользователи баз данных;
* пользовательские роли баз данных;
* перечень включенных функций;
* сетевые настройки.
* построение и управление иерархией групп информационных ресурсов;
* автоматическое определение типа и роли узла по результатам сканирования;
* построение и визуализацию в графическом интерфейсе пользователя схемы сети на уровне L3 модели OSI содержащей выявленные на момент проведения сканирования информационных ресурсов (серверы, АРМы, активное сетевое оборудование) и выявленные сетевые связи между ними;
* расчет сетевой достижимости между выбранными информационными ресурсами на схеме сети с учетом протоколов и портов;
* поиск информационных ресурсов в браузере информационных ресурсов графического интерфейса пользователя и на схеме сети;
* возможность задания информационным ресурсам уровня критичности и использование этой величины при количественной оценке опасности событий ИБ и инцидентов;
* возможность мониторинга доступности информационных ресурсов (узлов, сетевых сервисов и устройств);
* отслеживание изменений конфигурации информационных ресурсов и отображение истории изменения конфигурации информационного ресурса в графическом интерфейсе пользователя;
* объединение информационных ресурсов в динамические группы исходя из собранных данных по их конфигурации.

#### Подсистема должна обеспечивать выполнение следующих функций по сбору событий ИБ и обнаружению инцидентов ИБ:

* сбор и нормализацию событий ИБ из источников РСБ перечисленных в п.п. 4.4.1.3 настоящего ТЗ;
* нормализацию событий с использованием встроенных формул (приведение событий безопасности от различных источников РСБ к формату (таксономии) событий ПО MaxPatrol SIEM);
* агрегацию событий с использованием встроенных правил (объединение нескольких однотипных событий в одно событие);
* категоризацию событий;
* предоставление возможности создания пользователями собственных формул нормализации;
* хранение исходных и нормализованных событий;
* предоставление возможности формирования поисковых запросов в графическом интерфейсе пользователя к базе данных событий и возможности отфильтровать события по заданным критериям и сохранять результаты фильтрации для последующего быстрого доступа к интересующим событиям, при этом должна быть предусмотрена возможность создания иерархии фильтров с помощью папок;
* корреляцию событий и обнаружение (выявление) инцидентов ИБ;
* предоставление возможности создания пользовательских правил корреляции в том числе на основе встроенных системных правил;
* предоставление возможности управления списком активных правил корреляции с отображением статистики их срабатывания;
* обеспечение многоуровневой корреляции, когда результаты срабатывания правил корреляции подаются на вход другому правилу корреляции;
* использование табличных списков при формировании правил корреляции, и предоставление возможности их создания, удаления и редактирования через графический пользовательский интерфейс;
* функционал табличных списков должен позволять: реализовывать контроль времени жизни записей в таблице (TTL), индексацию выделенных колонок в целях ускорения доступа к записям, определение первичного ключа таблицы, импорт и экспорт всего содержимого табличного списка;
* при обращении к табличным спискам из правил корреляции должен быть доступен функционал: создания, обновления, удаления строк, а также очистки всей таблицы, обогащения корреляционного события найденными данными из табличного списка, выполнения математических функций инкремента, декремента, вычисления максимального, минимального и среднего при вставке данных в табличный список, выполнения математических функций вычисления максимального, минимального, среднего и подсчета общего числа строк при выборке данных из табличного списка;
* предоставление возможности задания правил обогащения событий, данными из табличных списков.

### Требования к подсистеме управления инцидентами информационной безопасности и данными об информационных ресурсах

#### Подсистема управления инцидентами ИБ и данными об информационных ресурсах (далее в пределах данного раздела – Подсистема) должна обеспечивать учет и обработку инцидентов ИБ на всех стадиях жизненного цикла инцидента, а также сбор и агрегацию сведений об информационных ресурсах и уязвимостях, которые ведутся в сторонних системах – источниках данных об информационных ресурсах, учет и обработку собранных списков данных об информационных ресурсах.

#### В части учёта и обработки собранных списков данных об информационных ресурсах должно обеспечиваться выполнение следующих функций:

* агрегация, в автоматическом режиме, инвентаризационной информации об информационных ресурсах и информации об уязвимостях программного обеспечения информационных ресурсов из источников, перечисленных в п.п. 4.4.2.1 настоящего ТЗ;
* импорт инвентаризационной информации из файлов Microsoft Excel в формате \*.xlsx;
* управление жизненным циклом информационных ресурсов;
* управление уязвимостями: индикация уязвимостей, сформированная на основе результатов сканирования MaxPatrol 8, уведомление о новых уязвимостях и об устранении уязвимостей по средствам почтовых сообщений, назначение задач по устранению уязвимостей и индикация их выполнения;
* обеспечение контроля структуры и состава компонентов ИВИ на основе сведений, полученных из источников данных об информационных ресурсах (Microsoft Active Directory, Microsoft System Center Configuration Manager, Kaspersky Security Center, MaxPatrol 8): появление новых устройств, установка или удаление программного обеспечения, изменение параметров безопасности, появление новых пользователей, контроль пакетов обновлений для ОС Windows (KB);
* учет информационных ресурсов и их свойств и взаимосвязей на основе сведений, полученных из источников данных об информационных ресурсах (Microsoft Active Directory, Microsoft System Center Configuration Manager, Kaspersky Security Center, MaxPatrol 8): сети, узлы сети, пользователи, группы, территориальный признак;
* учет и ведение карточек-описаний информационных ресурсов, отражающих их подробное описание и свойства, в том числе учет произвольных документов в карточке-описании (например, паспорт на систему, акт ввода в эксплуатацию, веб-ссылка на внешний ресурс), учет комментариев;
* возможность настраивать состав полей в карточке-описании информационного ресурса путем добавления собственных (пользовательских) полей;
* автоматическое включение оборудования в группы информационных ресурсов по настроенным правилам;
* журналирование событий, связанных с информационными ресурсами (добавление/удаление информационных ресурсов, добавление/удаление документов);
* визуализация связей между информационными ресурсами: отображение связи физических и информационных ресурсов (сети, узлы сети, пользователи, группы, территориальный признак).

#### В части учета и обработки инцидентов ИБ должно обеспечиваться выполнение следующих функций:

* автоматизация совместной деятельности работников (групп) Заказчика участвующих в процессе управления инцидентами ИБ в соответствии с разработанной в ходе проектирования ролевой моделью;
* регистрация в автоматическом режиме инцидентов ИБ по сообщениям от систем, перечисленных в п.п. 4.4.2.3 настоящего ТЗ;
* регистрация инцидентов вручную оператором (пользователем) Подсистемы через веб-интерфейс;
* формирование, ведение и учет карточек инцидентов;
* регистрация инцидентов посредством сбора почтовых сообщений с заданных почтовых ящиков и их разбора по регулярным выражениям или тегам;
* регистрация инцидентов посредством приема и обработки почтовых сообщений по протоколу SMTP без использования внешнего почтового сервера;
* регистрация, приоритезация инцидентов по степени критичности в автоматическом режиме;
* классификация инцидентов в соответствии с документом «Классификатор инцидентов информационной безопасности в ПАО «Транснефть» и организациях системы «Транснефть» (утвержден приказом ПАО «Транснефть» от 07.05.2018 № 68);
* управление жизненным циклом инцидентов, включая назначение статусов инцидентам в соответствии с документом «Классификатор инцидентов информационной безопасности в ПАО «Транснефть» и организациях системы «Транснефть» (утвержден приказом ПАО «Транснефть» от 07.05.2018 № 68);
* автоматизация функций по реагированию на инциденты: уведомление пользователей, назначение ответственных лиц, модификация инцидента (полей карточки инцидента), определение действий по инциденту (автоматическое создание задач при назначении действий по реагированию на инциденты), установка сроков по задачам, решение (предложение различных вариантов решения задачи пользователю), запуск скриптов автоматизации;
* наличие скриптов автоматизации (для ОС Windows/Linux) и набора команд (для сетевого оборудования Cisco и Huawei) для сбора релевантной информации по инцидентам   
  (в ходе работ по созданию САУСИБ могут быть проведены проверки применимости и нагрузки указанных скриптов на ИВИ Заказчика, данные проверки должны проводится по разработанному Исполнителем и согласованному и утвержденному Заказчиком плану тестирования);
* возможность настройки различных циклов обработки инцидентов ИБ в зависимости от типов инцидентов;
* возможность создания различных сценариев реагирования на разные типы инцидентов (Playbooks);
* возможность определения последовательности выполнения действий в сценариях реагирования;
* возможность формирования правил реагирования содержащих произвольный набор сценариев;
* возможность указания критериев в правилах реагирования, на основе которых выполняются сценарии. В качестве критериев должно выступать значение поля из карточки инцидента либо связанный информационных ресурс;
* возможность указания скрипта автоматизации при формировании сценария реагирования;
* графическое представление последовательности задач в сценарии реагирования;
* возможность учета уровня ущерба от реализации инцидентов информационной безопасности;
* привязка инцидентов к информационным ресурсам, индикация инцидентов на схеме сети на уровне L3 модели OSI;
* возможность создания групп/пользователей с доступом к инцидентам по определенной группе информационных ресурсов;
* формирование отчетности об инцидентах ИБ с возможностью сохранения отчётов в файлы в формате Microsoft Word, Microsoft Excel и в файлы в формате pdf, возможность настройки политик автоматической генерации и рассылки отчётов по электронной почте.

### Требования к подсистеме информационного обмена с ГосСОПКА

#### Подсистема информационного обмена с ГосСОПКА (далее в пределах этого раздела – Подсистема) должна обеспечивать выполнение следующих функций:

* учет и обработку сведений об инцидентах ИБ, полученных из подсистемы управления инцидентами ИБ и данными об информационных ресурсах;
* учет и обработку сведений об информационных ресурсах и уязвимостях программного обеспечения информационных ресурсов, полученных из подсистемы управления событиями ИБ и из подсистемы управления инцидентами ИБ и данными об информационных ресурсах;
* создание и изменение оператором в ручном режиме сведений об инцидентах ИБ, об информационных ресурсах и других сведений необходимых для осуществления информационного обмена с ГосСОПКА;
* передачу в ГосСОПКА в автоматизированном режиме, контролируемом по решению оператора Подсистемы (в соответствии с разработанной в ходе проектирования ролевой моделью), сведений о зафиксированных инцидентах ИБ, об информационных ресурсах, об уязвимостях программного обеспечения информационных ресурсов, о состоянии защищенности информационных ресурсов и пр.;
* получение запросов и информационных сообщений из ГосСОПКА.

#### Подсистема должна обеспечивать возможность информационного взаимодействия с ГосСОПКА как в ручном режиме (действия оператора), так и в автоматизированном режиме (посредством API).

#### Подсистема должна обеспечивать учет информационного обмена с ГосСОПКА. Факт получения информации должен подтверждается формированием и передачей соответствующего уведомления о её получении. В уведомлении должен содержаться уникальный идентификатор полученной информации.

#### Информационное взаимодействие с ГосСОПКА должно осуществляться в соответствии с техническими условиями, предоставленными Национальным координационным центром по компьютерным инцидентам (НКЦКИ).