Приложение 12

к [конкурсной документации](jl:34515777.4%20)

Техническая спецификация  
закупаемых товаров (заполняется заказчиком)

Наименование заказчика \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Наименование организатора

№ конкурса \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Наименование конкурса

№ лота \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Наименование лота

|  |  |
| --- | --- |
| Наименование кода Единого номенклатурного справочника товаров, работ, услуг\* | 801019.000.000010 |
| Наименование товара\* | Услуги по обеспечению информационной безопасности |
| Единица измерения\* | Услуга |
| Количество (объем)\* | 1 |
| Цена за единицу, без учета налога на добавленную стоимость\* | 38 690 124,00 |
| Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость\* | 38 690 124,00 |
| Срок поставки\* | 40 дней с момента даты подписания договора |
| Размер авансового платежа\* | 0% |
| Наименование национальных стандартов, а в случае их отсутствия межгосударственных стандартов на закупаемые товары. При отсутствии национальных и межгосударственных стандартов указываются требуемые функциональные, технические, качественные и эксплуатационные характеристики закупаемых товаров, с учетом нормирования государственных закупок. | **1. Наименование услуги**  Услуги Оперативного центра информационной безопасности (далее сокращенно – «Услуги ОЦИБ»).  **2. Основные термины и сокращения:**   * **ОЦИБ** - Оперативный центр информационной безопасности. Юридическое лицо или структурное подразделение юридического лица, осуществляющее деятельность по защите электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации на основании лицензии на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для оперативно-розыскных мероприятий. * **НКЦИБ** - Национальный координационный центр информационной безопасности РК. * **ИБ** - Информационная безопасность. * **Услуги ОЦИБ** - деятельность по обнаружению, оценке, прогнозированию, локализации, нейтрализации и профилактике угроз информационной безопасности информационно-коммуникационной инфраструктуры, объектов информатизации, подключенных к оперативному центру информационной безопасности. * **Дежурная смена мониторинга** - Круглосуточное обеспечение мониторинга и первичной обработки регистрируемых в системе ОЦИБ инцидентов силами Исполнителя в режиме 24/7. * **EPS (events per second)** - Количество событий в секунду. * **FPM (flow per minute)** - Количество сетевых пакетов в минуту. * **Технологическое окно** - Запланированный период времени для проведения технологических работ, в течение которого консоль системы будет недоступна. * **Простой** - Недоступность консоли управления системы для Заказчика. * **Источник событий** - Устройства Заказчика с настроенной системой логирования событий безопасности, например: сервер, сервис или приложение. * **Угроза ИБ** - потенциальная причина возникновения событий ИБ и инцидентов ИБ. * **Событие ИБ** - состояние объектов информатизации, свидетельствующее о возможном нарушении существующей политики безопасности либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности объектов информатизации. * **Инцидент ИБ** - отдельно или серийно возникающие сбои в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов. * **КВОИКИ** - Критически важные объекты информационно-телекоммуникационной инфраструктуры. * **Мониторинг событий информационной безопасности** - постоянное наблюдение за объектом информатизации с целью выявления и идентификации событий информационной безопасности.   **3. Цели закупаемых Услуг ОЦИБ**  Целями закупаемых услуг ОЦИБ являются:   1. Исполнение требований Закона «Об информатизации» ст.17 п2-1 пп1 о приобретении услуги оперативного центра информационной безопасности у третьих лиц и обеспечении подключения систем мониторинга обеспечения информационной безопасности к техническим средствам системы мониторинга обеспечения информационной безопасности Национального координационного центра информационной безопасности. 2. Приведение в соответствие с Постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности». 3. Повышение уровня защищенности ИТ-инфраструктуры и создание условий для предотвращения ущерба от инцидентов ИБ.   **4. Состав услуг ОЦИБ**   1. Мониторинг событий, связанных с нарушением ИБ и анализ результатов мониторинга в соответствии с п.38 Постановления Правительства Республики Казахстан от 20 декабря 2016 года № 832. 2. Мониторинг уязвимостей и анализ результатов мониторинга ИБ объектов информатизации Заказчика. 3. Внедрение системы по обнаружению вторжений следующего поколения.   **5. Требования к услугам**  Исполнитель оказывает услугу ОЦИБ в соответствии со статьями 7-2, 7-3 Закона РК «Об информатизации» и принимает на себя все обязательства, связанные с исполнением заявленных требований.   1. **Период оказания услуг**: с даты подписания договора по 31.12.2025. 2. **Обеспечение работоспособности платформы** со следующими параметрами:    * Период обслуживания платформы - 24/7/365;    * Количество технологических окон за месяц - не более 1;    * Уведомление о простоях - не более 60 минут;    * Максимальная длительность технологического окна - не более 6 часов;    * Уведомление о технологическом окне – не более чем за 3 рабочих дня. 3. **Технические и административные параметры оказываемых услуг**:    * Обработка и анализ поступающих событий ИБ и сетевых пакетов;    * Обрабатываемое количество событий в секунду – до 2000 EPS;    * Количество источников – неограниченно;    * Доступ к системе обработки событий для работников Исполнителя - не менее 10 пользователей;   **6. Описание услуг**  **6.1 Мониторинг событий, связанных с нарушением ИБ и анализ результатов мониторинга в соответствии с п.38 Постановления Правительства Республики Казахстан от 20 декабря 2016 года № 832.**   1. Настройка защищенного канала связи между Заказчиком и платформой ОЦИБ, проведение сетевых настроек и настроек безопасности. 2. Настройка источников событий на формирование событий безопасности в соответствии с форматами и типами записей, определенными с приложением №4 Приказа Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 марта 2018 года № 52/НҚ. 3. Разработка и адаптация правил корреляции событий под инфраструктуру Заказчика для нетиповых источников событий. 4. Мониторинг и анализ событий ИБ 24/7. 5. Информирование Заказчика о выявленных нарушениях и инцидентах ИБ с рекомендациями по локализации, для подтвержденных инцидентов ИБ. 6. Взаимодействие с НКЦИБ по обмену информацией, необходимой для обеспечения ИБ объектов информатизации, угрозами и инцидентам ИБ. 7. Организация сбора, консолидации и хранения событий безопасности в течение периода, определенного законодательными требованиями (3 мес. - оперативный доступ, 3 года – архивный) на стороне Заказчика. 8. Круглосуточный прием и регистрация обращений Заказчика. 9. Заказчик определяет список источников, подлежащих мониторингу, который закрепляется документом с подписями обеих сторон   **6.2 Мониторинг уязвимостей и анализ результатов мониторинга**   1. Развертывание и настройка на стороне Заказчика сканера безопасности. 2. Сканирование сети на уязвимости согласованного совместно с Заказчиком списка источников. 3. Анализ и оценка сведений по результатам сканирования, классификация уязвимостей, рекомендации по устранению, отчет о выявленных уязвимостях и мерах их устранения. 4. Направление отчета Заказчику. 5. Круглосуточный прием и регистрация обращений Заказчика   **6.3 Мониторинг системы обнаружения вторжений следующего поколения**   1. Развертывание и настройка системы обнаружения вторжений следующего поколения. 2. Создание уникальных ловушек после предоставления данных по подключенным источникам и сети инфраструктуры Заказчика. 3. Мониторинг системы обнаружения вторжений следующего поколения. 4. Анализ и оценка сведений по обнаруженным инцидентам в зоне системы по обнаружению вторжений следующего поколения 5. Направления отчета по обнаружениям по требованию Заказчика 6. Круглосуточный прием и регистрация обращений Заказчика   **7. Требования к организации группы мониторинга**   * 1. **Непрерывный мониторинг**: в соответствии с Едиными требованиями в области информационно-коммуникационных технологий и обеспечения информационной безопасности Республики Казахстан, постановлением Правительства от 20 декабря 2016 года № 832, организация постоянного мониторинга информационной безопасности является обязательной. Мониторинговая группа должна функционировать круглосуточно (24/7) для обеспечения контроля событий информационной безопасности, что включено в требования по управлению безопасностью информационно-коммуникационных систем.   2. **Количество сотрудников**: Группа мониторинга должна работать в круглосуточном режиме (24/7) с достаточным количеством сотрудников для выполнения непрерывных функций, при этом соблюдая нормы рабочего времени, согласно Трудовому кодексу РК.   3. **Требование к территориальному присутствию Исполнителя:** Исполнитель должен иметь представительства в следующих **регионах Казахстана** для обеспечения оперативного реагирования на инциденты:   г. Алматы, г. Астана, г. Актау, г. Актобе, г. Атырау, г. Жезказган, г. Караганда, г. Кокшетау, г. Костанай, г. Кызылорда, г. Павлодар, г. Петропавловск, г. Семей, г. Талдыкорган, г. Тараз, г. Уральск, г. Усть-Каменогорск, г. Шымкент, г. Туркестан.  **Оперативное реагирование** – Исполнитель должен обеспечить время прибытия специалистов в региональные подразделения Заказчика в течение **1 часа** с момента подтверждения инцидента.  **Штатная техническая поддержка** – В каждом регионе должно быть не менее **одного специалиста**, обладающего знаниями и компетенциями для выполнения сервисных работ.  **Подтверждение наличия представительств** – В составе конкурсной заявки Исполнитель должен предоставить:  Список представительств Исполнителя с адресами и контактными данными.  **8. Требования к системам защиты информации**   * 1. **Требование к системе по обнаружению вторжений следующего поколения**   1. Предоставляемое решение должно быть развернуто без необходимости реорганизации существующей топологии сети конечного пользователя.  2. Предоставляемое решение должно включать как минимум следующие модули:  a. Узел центрального управления,  b. Узел ловушек (который запускает приманки),  c. Агент на конечных устройствах (крошки приманки).  3. Предоставляемое решение должно иметь возможность размещения пассивных ложных данных (крошки, приманки) на реальных сетевых хостах с операционными системами Linux и Microsoft Windows.  4. Предоставляемое решение должно масштабироваться без необходимости повторной установки компонентов системы.  5. Предоставляемое решение должно поддерживать архитектуру с множеством экземпляров узлов ловушек (приманок) с выделенным функциональным экземпляром для поддержки операций управления.  6. Предоставляемое решение должно иметь возможность размещения симуляционных ловушек (приманок) в разных сетевых сегментах.  7. Предоставляемое решение должно работать без необходимости использования в качестве входных данных любой информации о потоке IP-трафика (например, сырые копии сетевого IP-трафика, NetFlow, sFlow, jFlow и т.д.).  Требования к управлению:  8. Предоставляемое решение должно иметь интуитивно понятный интерфейс и не требовать значительных затрат на его обслуживание и поддержку.  9. Предоставляемое решение должно поддерживать мультитенантность, что означает возможность создания изолированных друг от друга сред, которые управляются в рамках одной консоли.  10. При этом администраторы отдельных тенантов имеют доступ только к настроенному для них сегменту сети в консоли управления, а главный администратор имеет доступ ко всем аккаунтам.  11. Предоставляемое решение должно поддерживать RBAC (Role-Based Access Control, Ролевое управление доступом) для предоставления прав системным администраторам.  12. Предоставляемое решение должно вести детальный аудит всех действий в модуле управления. Когда вносятся изменения в настройки, журнал аудита должен четко фиксировать начальные и конечные значения изменяемых параметров.  13. Предоставляемое решение должно поддерживать мультифакторную аутентификацию (MFA). Обязательна поддержка алгоритма одноразовых паролей с привязкой ко времени (TOTP).  14. Предоставляемое решение должно иметь возможность создания архива логов для автономного устранения технических проблем службой поддержки поставщика.  Функциональные требования:  15. Каждая ловушка (приманка) должна быть уникальной, с собственным набором характеристик (MAC-адрес, IP-адрес, имя хоста, имитируемые службы и настройки).  16. Ловушки не должны использовать опцию масштабирования на основе IP-алиасов, когда у каждой ловушки несколько IP-адресов, что значительно упрощает обнаружение похожих ловушек для злоумышленников в инфраструктуре.  17. Предоставляемое решение должно иметь возможность создавать ловушки, которые периодически:  a. подключаются к внешним веб-ресурсам,  b. выполняют разрешение имен хостов и доменных имен через DNS, mDNS, LLMNR и NetBIOS,  c. запрашивают список файловых ресурсов через протокол SMB.  18. Предоставляемое решение должно предоставлять возможность создавать и распространять фальшивые данные (breadcrumbs) на реальных конечных узлах сети в производственной среде.  19. Типы фальшивых данных должны включать как минимум:  a. сохраненные данные для автологина,  b. профили подключений к имитируемым источникам данных,  c. сетевые ресурсы,  d. сохраненные сессии RDP и SSH,  e. конфигурационные файлы с учетными записями для имитируемых баз данных и др.  20. Предоставляемое решение должно включать инструменты для распределения и создания фальшивых кешированных данных на хостах рабочих станций.  21. Предоставляемое решение должно обнаруживать сетевые вторжения (обнаружение атак типа brute force, попытки подключиться к службам на имитациях) и классифицировать их критичность, независимо от типа и принципа реализации угрозы. Обнаружение и классификация должны применяться как к незашифрованному, так и к зашифрованному трафику.  22. Предоставляемое решение должно отображать историю подключений к ловушкам и историю манипуляций злоумышленника с ловушкой:  a. с указанием IP-адреса скомпрометированного хоста,  b. скомпрометированных учетных данных,  c. протоколов/портов взаимодействия.  23. Предоставляемое решение должно иметь встроенные графические панели, отображающие статистику работы системы, событий и др.  24. Предоставляемое решение должно обнаруживать атаки типа MiTM (человек посередине), включая:  a. ARP spoofing,  b. отравление NBT/LLMNR/mDNS,  c. перехват HTTPS-запросов.  25. Предоставляемое решение должно иметь возможность создания ловушек в полностью автоматическом режиме.  26. Предоставляемое решение должно включать как минимум следующий список типов ловушек:  a. сервер Microsoft RDP,  b. сервер файлов Microsoft SMB,  c. ловушка Microsoft MS RPC для обнаружения попыток подключения MS RPC,  d. серверы с ОС Linux,  e. веб-интерфейс пользователя QRadar,  f. веб-интерфейс VMware ESX,  g. веб-интерфейс Fortinet,  h. веб-интерфейс пользователя Microsoft Outlook Web Access,  i. SCADA/HMI/PLC,  j. сервер DNS,  k. сервер MySQL,  l. сервер PostgreSQL,  m. файловый сервер FTP,  n. файловый сервер Samba,  o. сервер Modbus TCP,  p. брокер MQTT.  27. Предоставляемое решение должно иметь возможность создания сетевых ловушек на основе любого веб-сайта/веб-сервиса, используемого в сети клиента. Эти ловушки должны содержать известные уязвимости веб-сервисов (OWASP TOP 10).  28. Веб-ловушки должны иметь следующие параметры конфигурации:  a. заголовок сервера для имитации различных веб-серверов,  b. ограничение скорости для предотвращения DoS-атак на ловушку,  c. допустимые HTTP-методы,  d. настраиваемые пути и файлы на таких ловушках, включая ответ,  e. добавление произвольных HTTP-заголовков,  f. TLS-сертификат для веб-ловушки.  29. Предоставляемое решение должно иметь возможность регенерации файлов-приманок, включая воссоздание сетевых приманок для обеспечения согласованности и достоверности содержимого этих файлов-приманок.  30. Ловушки OT должны имитировать веб-интерфейсы SIEMENS и Allen-Bradley от Rockwell Automation PLC.  31. Ловушки OT должны поддерживать протоколы S7comm и Modbus TCP.  32. Предоставляемое решение должно точно классифицировать и объединять события, связанные с обнаруженной атакой, в одно уведомление, чтобы не перегружать операторов системы множеством событий для просмотра и обработки.  33. Предоставляемое решение должно предоставлять возможность создавать собственные типы сетевых ловушек на основе существующих в системе базовых типов. После создания нового типа ловушки пользователь должен иметь возможность автоматически создавать более одной ловушки выбранного типа сразу без дополнительных манипуляций. Конфигурации новых типов ловушек должны быть в простой и стандартизированной текстовой форме (YAML или JSON).  34. Предоставляемое решение должно иметь встроенную функциональность IRMS (система управления инцидентами безопасности) с указанием статуса каждого обработанного уведомления.  35. Ловушки с высоким уровнем взаимодействия должны обеспечивать интерактивность как минимум на уровне ответа на сканирование, запроса учетных данных и отображения графического и/или текстового интерфейса. Каждая ловушка должна быть уникальной, со своим IP-адресом, без использования IP-алиасов и технологии Full OS.  36. Предоставляемое решение должно использовать метод обнаружения киберугроз без использования сигнатур.  37. Предоставляемое решение должно иметь возможность построения и визуализации взаимодействия сетевых активов друг с другом.  38. Предоставляемое решение должно создавать дамп сетевого трафика, связанный с уведомлениями о безопасности. Дамп сетевого трафика должен быть в формате PCAP.  39. Программная платформа должна иметь возможность добавления легитимных сервисов  **8.2 Требования к управлению уязвимостями**   1. Система должна обеспечивать процесс управления уязвимостями для не менее 1024 активов сети. 2. Система должна обеспечивать сканирование с целью инвентаризации активов для неограниченного количества активов. 3. Информация об уязвимостях должна быть доступной через интерфейс SIEM системы без необходимости установки дополнительных приложений или расширений. 4. Система управления уязвимостями должна использовать данные с SIEM системы и системы управления конфигурациями для обеспечения приоритезации процесса исправления уязвимостей. 5. Данные о найденных уязвимостях должны автоматически влиять на срабатывание корреляционных правил SIEM для выявления инцидентов. 6. Каждая уязвимость должна быть автоматически закреплена за владельцем актива и должна предоставляться возможность задания интервала времени на исправление найденной уязвимости и автоматической проверки её устранения. Владелец актива должен быть уведомлен через: электронную почту или интерфейс SIEM системы. 7. Система должна предоставить возможность автоматически запускать процесс сканирования при: любых событиях/инциденте информационной безопасности, выявления нового актива в сети на основе данных из: журналов событий (logs), данных по NetFlow, данных с jFlow, данных по sFlow, данных IPFIX, изменения конфигурации ОС актива, или создание новой учетной записи на уровне ОС актива. 8. Система должна обеспечить функционал внутреннего и внешнего сканирования инфраструктуры по расписанию. 9. Политики сканирования должны устанавливаться по типу сканирования (Web Scan, Patch Scan, Discovery Scan, Database Scan, Full Scan), также возможность создавать новые политики сканирования или собственные шаблоны. 10. Тип сканирования должен быть определен: протоколом проведения сканирования, диапазоном портов сканирования, и группами активов сканирования. 11. Система управления уязвимостями должна предоставлять возможность задавать параметры запуска сканирования по расписанию и автоматического получения информации для следующих сканеров путем инфраструктурной интеграции через веб-интерфейс без необходимости запуска и использования сторонних приложений, баз данных, дополнительных интерфейсов, окон или других виртуальных устройств: IBM Guardium, AXIS Scanner, Beyond Security AVDS, Digital Defense inc. AVS, eEye REM Scanner, FoundScan Scanner, SiteProtector, BigFix, Juniper NSM Profiler, McAfee VM, Microsoft SCCM, nCircle IP360 Scanner, Nessus Scanner, NMap Scanner, Outpost24 Vulnerability Scanner, Positive Technologies MaxPatrol, Qualys Detection Scanner, Qualys Scanner, Rapid7 NexPose Scanner, Saint Scanner, SecureScout Scanner, Tenable Security Center. 12. При сканировании веб-приложений использовать эвристические методы анализа, позволяющие обнаруживать уязвимости в соответствии с таксономиями Open Web Application Security Project TOP 10. 13. Через единый интерфейс SIEM системы пользователь должен иметь возможность: 14. Запускать сканирование устройств, веб-приложений, подсетей и внешнего периметра. 15. Настраивать гибкие сценарии сканирования для устройств, веб-приложений, подсетей и внешнего периметра, например: сканирование каждые 3 суток, в 13:00 часов. 16. Настраивать "глубину сканирования", например - с использованием полномочий администратора или без.     1. **Требования к сканеру уязвимостей**   **Общие требования**   1. Сканер уязвимостей должен иметь полную видимость активов и уязвимостей в одной платформе. 2. Должна быть возможность идентификации всех активов в сети, включая физические устройства, виртуальные машины, облачные ресурсы, контейнеры и IoT-устройства. 3. Сканер уязвимостей должен иметь функционал автоматически обнаруживать новые активы в сети и добавлять их в инвентаризацию. 4. Платформа должна поддерживать интеграцию с системами управления конфигурацией (CMDB), SIEM и ITSM. 5. У сканера должны быть доступны регулярные обновления базы данных уязвимостей для обеспечения актуальности и использования актуальных технологий. 6. Иметь возможность поддержки сквозной интеграции для управления жизненным циклом уязвимостей — от обнаружения до устранения. 7. Возможность неограниченного инвентаризационного сканирования сети как по расписанию, так и по требованию 8. Возможность сканирования на уязвимости как с помощью агентов, так и в безагентном режиме 9. Возможность проведения сканирования сети на уязвимости как по расписанию, так и по требованию 10. Предоставление доступа к базе уязвимостей, с описанием уязвимостей, а также с рекомендациями по их устранению 11. Возможность сканирования на уязвимости периметра из датацентра Платформы 12. Для безагентного сканирования должна быть возможность задавать профили сканирования, в которых должна быть возможность установить (как минимум):     1. Интенсивность сканирования     2. Сканирование определённых портов     3. Использование учётной записи     4. Брутфорс учётных записей     5. Выбор уязвимостей для сканирования 13. Возможность проведения анализа инфраструктуры на новые уязвимости без необходимости пересканирования инфраструктуры (на основании исторических данных) 14. Для безагентного сканирования внутренней корпоративной сети должна использоваться защищённая виртуальная машина(ы) 15. Возможность проверки наличия стандартных паролей на оборудовании 16. 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 17. 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 18. 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) 19. В Платформе должен быть разделён процесс сканирования от процесса создания отчётов: все сканирования должны наполнять центральную базу по уязвимостям 20. Система должна отслеживать статус уязвимости в инфраструктуре и время нахождения в инфраструктуре 21. Система должна предоставлять как минимум следующие статусы для уязвимостей в инфраструктуре:     1. новая уязвимость (обнаружена 1 раз)     2. известная уязвимость (обнаружена 2+ раза)     3. исправленная уязвимость (была новой/известной, но система перестала обнаруживать её в инфраструктуре)     4. заново открытая уязвимость (была исправленной, но снова появилась в инфраструктуре) 22. Платформа должна позволять обеспечивать непрерывное сканирование критических ресурсов 24/7/365 23. 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  1. Возможность автоматической динамической маркировки устройств на базе предустановленных пользователем правил:    1. По принадлежности к IP подсети    2. На базе парсинга NetBIOS и FQDN имени    3. На базе операционной системы    4. По открытым портам/сервисам    5. По наличию конкретной уязвимости    6. На основании сроков сканирования 2. Маркировка должна поддерживать древовидные структуры маркеров с наследованием 3. Возможность формирований отчетов как по расписанию, так и по требованию 4. Возможность настройки отчётов согласно требованиям компании 5. Отчет может / должен содержать следующую информацию:    1. Название уязвимости и уровень ее критичности по шкале вендора и по CVSS    2. Перечень уязвимых систем или сервисов    3. Статус уязвимостей (новая / активная / исправленная)    4. Рекомендации по устранению уязвимости, или ссылку на патч, если таковой существует    5. Дополнительные критерии для приоритезации уязвимости: наличие эксплойта, вредоносного кода, и тд. 6. Платформа должна предоставлять возможность фильтрации отчётов по конкретному типу уязвимостей:    1. На базе наличия патча    2. На базе наличия эксплоита в конкретных эксплоит-паках    3. Наличия вредоносного кода для уязвимости    4. CVSS рейтингу (CVSSv2, CVSSv3)    5. Вектору атаки CVSS    6. Вендору и продукту    7. Критичности уязвимости    8. CVE ID    9. И тд. 7. Система отчётности должна предоставлять возможность создания тикетов и назначения их на определённых людей 8. Отчеты для руководства. Краткое представление информации с построением графических трендов по результатам сканирования и выявлению или устранению уязвимостей 9. Отчёты для IT специалистов по обновлениям, а не по уязвимостям 10. Отчёты по успешности прохождения аутентификации при безагентном сканировании систем 11. Система должна предоставлять аналитику по обнаруженным уязвимостям и средства для приоритезации устранения уязвимостей 12. Система должна предоставлять возможность формировать динамический отчет для приоритезации угроз, с указанием хостов, уязвимостей и необходимых обновлений на основе следующих данных:     1. Время нахождения уязвимости в инфраструктуре     2. Время публикации уязвимости     3. Наличие следующих векторов атак:        1. Запущенный сервис        2. Активное ядро системы        3. Устранение уязвимости путем изменения конфигурации        4. Обнаружение уязвимости путем удаленного сканирования        5. Устройство с публичным IP адресом     4. Наличие следующих индикаторов угроз:        1. Лёгкая возможность эксплуатации уязвимости        2. Отсутствие патча для уязвимости        3. Риск потери данных при эксплуатации уязвимости        4. Наличие публичного эксплоита        5. Наличие вредоносного кода для уязвимости        6. Риск отказа в обслуживании (DoS) при эксплуатации уязвимости        7. Уязвимость активно используется в атаках        8. Наличие эксплоита в публичных эксплоит-паках        9. Риск быстрого распространения внутри инфраструктуры        10. Уязвимость используется для повышения привилегий        11. Уязвимость используется для выполнения произвольного кода 13. Система должна в реальном времени показывать статус защищённости ресурсов компании (посредством предустановленных дешбордов) 14. Система должна позволять пользователям создавать свои виджеты для дэшбордов 15. Система должна обеспечивать возможность выгрузки дэшбордов и виджетов 16. Система отчётности должна обеспечивать возможность сквозного поиска по всем проанализированным ресурсам 17. Возможность маркировки уязвимости (в случае ложного срабатывания) с последующим исключением из отчётов   **Функциональные требования**   1. Платформа должна поддерживать проведение инвентаризации активов в режиме реального времени с использованием пассивного мониторинга и агентного подхода. 2. Система должна иметь функционал автоматически определять приоритет уязвимостей на основе следующих факторов: 3. Уровень риска (CVSS v2/v3). 4. Наличие и популярность эксплойтов. 5. Контекст бизнес-критичности активов. 6. Потенциальное воздействие на бизнес. 7. Реализована возможность отслеживания исправления уязвимостей с использованием автоматизированных процессов (Remediation Workflow). 8. Отчеты о состоянии безопасности должны включать метрики, аналитику и прогнозные модели для оценки эффективности управления уязвимостями. 9. Поддержка внешнего и внутреннего сканирования инфраструктуры по расписанию или по запросу. 10. Возможность идентификации и управления лицензиями программного обеспечения на каждом активе. 11. Функционал автоматической классификации активов по назначению, типу и бизнес-критичности. 12. Функционал создания сценариев автоматизации исправления уязвимостей с интеграцией в процессы управления патчами (Patch Management). 13. Функционал выявления конфигурационных уязвимостей на основе стандартов безопасности. 14. Функционал анализа зависимости уязвимостей от используемых библиотек и сторонних компонентов программного обеспечения. 15. Функционал выявления вредоносного ПО и угроз в рамках процессов защиты. 16. Система должна использовать комплексную информацию об угрозах и эксплойтах для автоматической оценки реального уровня риска на основе нескольких факторов, включая зрелость кода эксплойта, активное использование уязвимости в реальной среде, критичность актива и его местоположение. 17. Система должна предоставлять возможность обнаружения, управления и устранения уязвимостей в кастомных разработках и программном обеспечении с использованием собственных логик и подписей угроз.   **Технические требования**   1. Поддержка сканирования по всем основным протоколам (TCP, UDP, HTTP, HTTPS и др.). 2. Настройка глубины сканирования, включая сканирование с полномочиями администратора или без них. 3. Возможность создания пользовательских политик и шаблонов сканирования. 4. Использование эвристических методов анализа для обнаружения уязвимостей в веб-приложениях. 5. Визуализация данных на сводных дашбордах, включая состояние активов, уязвимостей и прогресс исправлений. 6. Анализ трендов и прогнозирование рисков на основе исторических данных. 7. Автоматическая оценка воздействия уязвимости на активы и подсети сети. 8. Прогнозирование времени и ресурсов, необходимых для исправления уязвимостей. 9. Поддержка работы агентного подхода для постоянного мониторинга активов.   **Пользовательский интерфейс**   1. Интуитивно понятный интерфейс с доступом к ключевым функциям через единое окно управления. 2. Настройка гибких сценариев сканирования (например, анализ каждые три дня в заданное время). 3. Уведомления о найденных уязвимостях через электронную почту, мессенджеры и другие системы оповещения. 4. Возможность создания кастомизированных отчетов с фильтрами, пользовательскими полями и визуализацией. 5. Автоматическая отправка отчетов ответственным лицам по расписанию. 6. Настройка сценариев реагирования на обнаруженные уязвимости, включая активацию сканирования после изменений в конфигурации системы.   **Безопасность и соответствие**   1. Соответствие международным стандартам безопасности, включая ISO/IEC 27001. 2. Поддержка шифрования данных при передаче и хранении. 3. Реализованы функции аудита и логирования всех операций. 4. Доступность API для интеграции с кастомными инструментами и автоматизации управления уязвимостями.   **Производительность и масштабируемость**   1. Поддержка работы в крупных сетях. 2. Возможность распределенного сканирования для снижения нагрузки на сеть. 3. Высокая скорость сканирования с минимальным воздействием на производительность сети.   **Поддержка и обслуживание**   1. Круглосуточная техническая поддержка от поставщика. 2. Доступ к детальной документации, включая руководство пользователя, технические спецификации и обучающие материалы. 3. Автоматическое обновление программного обеспечения и базы данных уязвимостей. 4. Поддержка пользовательских форумов и ресурсов для обучения (вебинары, базы знаний).   **9. Требования к Исполнителю**   * 1. Исполнитель должен предоставить сертификаты соответствия стандартам ISO/IEC 27001, выданные аккредитованными органами, что подтверждает компетентность компании в области управления безопасностью данных.   2. Исполнитель обязан предоставлять ежемесячные отчеты о проделанной работе, в которых должны быть расписаны выявленные инциденты, статистика обработки событий и рекомендованные меры по повышению уровня безопасности. Также прилагается сменный график сотрудников, который включает в себя ФИО сотрудника, дату и время смены.   3. Исполнитель осуществляет мониторинг событий и анализ инцидентов информационной безопасности, используя средства защиты информации, предоставленные Заказчиком.   4. Исполнитель совместно с Заказчиком обеспечивает организацию защищенного VPN-туннеля к средствам защиты информации, предоставленные Заказчиком.   **10. Предоставление данных для расследований инцидентов ИБ**  При обработке инцидента ИБ ответственный за расследование инцидента ИБ сотрудник Исполнителя проводит сбор информации по инциденту у Заказчика, который предоставляет следующие данные: 10.1 Филиал, регион, в котором зафиксирован инцидент. 10.2 Время возникновения инцидента. 10.3 ИС, IP-адреса, MAC-адреса, FQDN-имена хостов, относящихся к инциденту. 10.4 Контактные данные сотрудника (ФИО, телефон, адрес электронной почты), ответственного за эксплуатацию систем, которые относятся к инциденту. 10.5 Критичность инцидента.  **11. Проведение расследований инцидентов ИБ**  После сбора первичной информации по инциденту ответственный за расследование инцидента ИБ приступает к сбору расширенной информации по инциденту, которая включает в себя: 11.1 Сбор дополнительных данных о фигурантах инцидента (события с фигурантами в других информационных, инфраструктурных системах, системах защиты информации за предшествующий период от 1 месяца; имеющиеся доступы/роли/привилегии; наличие ранее зафиксированных инцидентов ИБ). 11.2 Сбор дополнительных данных о системах - участниках инцидента (зафиксированные события и инциденты ИБ, результаты автоматизированных сканирований, проверок и аудитов). 11.3 Другая дополнительная информация, связанная с инцидентом ИБ.  Данная работа ведётся совместно с Заказчиком. Качество расследования зависит от данных, предоставляемых Заказчиком.  11.4 По результатам собранной информации проводится расследование инцидента ИБ. В процессе расследования инцидента сотрудник Исполнителя устанавливает:   * Хронологию событий, повлекших за собой возникновение инцидента ИБ. * Причины, из-за которых возник инцидент ИБ. * Ложность или истинность инцидента ИБ. * Последствия инцидента ИБ.   11.5 По итогам расследования инцидента ИБ формируется отчёт о проделанной работе. Исполнитель, помимо анализа инцидента и установления источника и причин, формирует набор технических рекомендаций, позволяющих предотвратить или снизить вероятность возникновения аналогичных инцидентов в дальнейшем. 11.6 Заказчик анализирует предоставленную ему информацию, принимает решение о применимости выданных рекомендаций в своей инфраструктуре и проводит предложенные технические мероприятия. 11.7 Предложенный механизм предотвращения анализируется Исполнителем и Заказчиком на возможность повторного применения при возникновении инцидента и фиксируется в документации, описывающей профиль системы.  **12. Подключение новых источников к системе ОЦИБ**  Заказчик инициирует запрос на подключение дополнительного источника событий ИБ, предоставляя следующую информацию: 12.1 Тип источника. 12.2 Информация по получению данных с источника (IP-адрес, данные доступа). 12.3 Список сценариев обнаружения инцидентов, которые необходимо контролировать в рамках данного источника. 12.4 Дополнительная информация, необходимая для определения системы в сценариях обнаружения инцидентов.  12.5 Исполнитель, совместно со специалистами Заказчика, оценивает техническую возможность сбора требуемых событий с целевого источника и согласовывает механизм и способ подключения. 12.6 Исполнитель оценивает достаточность предоставленной информации для выполнения работ и вносит изменения в сценарии обнаружения инцидентов с учетом подключения нового источника. 12.7 Исполнитель и сотрудники Заказчика выполняют требуемые настройки на системе сбора событий ИБ и источнике для его подключения. 12.8 По завершению подключения и проверки работоспособности Исполнителем совместно с Заказчиком оформляется акт проделанных работ с подписью двух сторон  **13. Отключение источника от системы ОЦИБ**  Сотрудник Заказчика инициирует запрос на отключение источника, предоставляя следующую информацию: 13.1 Тип источника. 13.2 Идентификатор источника (IP-адрес, приложение).  13.3 Исполнитель проводит анализ существующих сценариев обнаружения инцидентов и информирует сотрудников Заказчика в случае, если отключение источника приводит к их модификации либо исключению из списка контролируемых инцидентов. 13.4 В случае необходимости Исполнитель и сотрудник Заказчика выполняют работы по изменению состава инцидентов на системе сбора событий ИБ и источнике для его отключения. 13.5 По завершению отключения и проверки работоспособности Исполнителем совместно с Заказчиком оформляется акт проделанных работ с подписью двух сторон  **14. Реализация новых правил обнаружения инцидентов**  14.1 Заказчик при необходимости инициирует запрос на реализацию нового правила (не более 60) обнаружения инцидентов ИБ, предоставляя следующую информацию:   * Общее описание и критерии возникновения инцидента. * Тип источников данных для выявления инцидента. * Плановая критичность инцидента.   14.2 Исполнитель анализирует техническую возможность реализации правила в рамках инфраструктуры Заказчика в системе ОЦИБ, привлекая специалистов Заказчика для более детальной проработки сценария угроз возникновения инцидентов ИБ. 14.3 Исполнитель и сотрудники Заказчика согласовывают итоговый сценарий обнаружения инцидента по новому правилу, определяют его критичность и процесс взаимодействия по инциденту. 14.4 Исполнитель выполняет работы по реализации нового правила, производя настройки системы ОЦИБ. 14.5 По завершению настройки и проверки работоспособности Исполнителем совместно с Заказчиком закрепляется акт проделанных работ с подписями обеих сторон.  Стоимость услуг по обеспечению информационной безопасности не более 3 224 177,00 тенге без НДС в месяц |
| Год выпуска | 2025 |
| Гарантийный срок (в месяцах) | 12 месяцев |
| Описание требуемых функциональных, технических, качественных, эксплуатационных и иных характеристик закупаемого товара |  |
| Сопутствующие услуги (указываются при необходимости) (монтаж, наладка, обучение, проверки и испытания товаров) | Поставщик обязан произвести установку (удаленную) и настройку на сервеном оборудовании. |
| Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора о государственных закупках (указываются при необходимости) (Отклонение потенциального поставщика за не указание и непредставление указанных сведений не допускается) |  |

\* сведения подтягиваются из плана государственных закупок (отображаются автоматически).

Примечание.

1. Каждое требование по функциональным, техническим, качественным, эксплуатационным, иным характеристикам, сопутствующим услугам и дополнительным условиям к исполнителю указывается отдельной строкой.

2. Установление в настоящей технической спецификации квалификационных требований, предъявляемых к потенциальному поставщику, не допускается.

3. Установление требований технической спецификации в иных документах не допускается.

Конкурстық [құжаттамаға](jl:31968033.4%20)

12-қосымша

Сатып алынатын тауарлардың техникалық ерекшелігі

(тапсырыс беруші толтырады)

Тапсырыс берушінің атауы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ұйымдастырушының атауы

Конкурстың № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Конкурстың атауы

Лоттың № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Лоттың атауы

|  |  |
| --- | --- |
| Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы\* | 801019.000.000010 |
| Тауардың атауы\* | Бағдарламалық қамтамасыз етуді пайдалану құқығына лицензия беру бойынша қызметтер |
| Өлшем бірлігі\* | қызмет |
| Саны (көлемі)\* | 1 |
| Қосымша құн салығын қоспағанда, бірлік бағасы \* | 38 690 124,00 |
| Қосымша құн салығын қоспағанда, сатып алуға бөлінген жалпы сома\* | 38 690 124,00 |
| Жеткізу мерзімі\* | Шартқа қол қойылған күннен бастап 40 күн |
| Аванстық төлем мөлшері\* | 0% |
| Ұлттық стандарттардың атауы, ал олар болмаған жағдайда сатып алынатын тауарларға мемлекетаралық стандарттар. Ұлттық және мемлекетаралық стандарттар болмаған кезде Мемлекеттік сатып алуды нормалауды ескере отырып, сатып алынатын тауарлардың талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары көрсетіледі. | 1. Қызмет атауы  Ақпараттық қауіпсіздіктің жедел орталығының қызметтері (бұдан әрі қысқартылған - "ОЦИБ қызметтері").  2. Негізгі терминдер мен қысқартулар:  \* ОЦИБ-ақпараттық қауіпсіздіктің жедел орталығы. Электрондық ақпараттық ресурстарды, Ақпараттық жүйелерді, телекоммуникация желілерін және басқа да ақпараттандыру объектілерін қорғау жөніндегі қызметті жедел-іздестіру іс-шараларына арналған ақпараттың ағып кетуінің техникалық арналарын және арнайы техникалық құралдарды анықтау жөніндегі қызметтер көрсетуге арналған лицензия негізінде жүзеге асыратын заңды тұлға немесе заңды тұлғаның құрылымдық бөлімшесі.  \* ҰҚКҰК-ҚР Ұлттық ақпараттық қауіпсіздікті үйлестіру орталығы.  \* АҚ - Ақпараттық қауіпсіздік.  \* ОӘБ қызметтері-ақпараттық-коммуникациялық инфрақұрылымның, ақпараттық қауіпсіздіктің жедел орталығына қосылған ақпараттандыру объектілерінің ақпараттық қауіпсіздігіне төнетін қатерлерді анықтау, бағалау, болжау, оқшаулау, бейтараптандыру және алдын алу жөніндегі қызмет.  \* Мониторингтің кезекші ауысымы-24/7 режимінде Орындаушының күшімен ОЦИБ жүйесінде тіркелген оқиғалардың мониторингін және бастапқы өңдеуін тәулік бойы қамтамасыз ету.  \* EPS (events per second) - секундына оқиғалар саны.  • FPM (flow per minute) - минутына желілік пакеттер Саны.  \* Технологиялық терезе-жүйенің консолі қолжетімсіз болатын технологиялық жұмыстарды жүргізу үшін жоспарланған уақыт кезеңі.  \* Қарапайым-Тапсырыс беруші үшін жүйенің басқару консолі қол жетімді емес.  \* Оқиға көзі-сервер, сервис немесе қосымша сияқты қауіпсіздік оқиғаларын тіркеу жүйесі конфигурацияланған Тапсырыс берушінің құрылғылары.  \* АҚ қаупі-АҚ оқиғалары мен ақ инциденттерінің пайда болуының ықтимал себебі.  \* АҚ оқиғасы-ақпараттандыру объектілерінің жай-күйі, қолданыстағы қауіпсіздік саясатының бұзылуы немесе ақпараттандыру объектілерінің қауіпсіздігіне қатысы болуы мүмкін бұрын белгісіз жағдай туралы куәландырады.  \* АҚ инциденті-ақпараттық-коммуникациялық инфрақұрылымның немесе оның жекелеген объектілерінің жұмысында олардың тиісінше жұмыс істеуіне қауіп төндіретін және (немесе) электрондық ақпараттық ресурстарды заңсыз алу, көшіру, тарату, өзгерту, жою немесе бұғаттау үшін жағдайлар жасайтын жеке немесе сериялық туындайтын іркілістер.  \* КВОИКИ-ақпараттық-телекоммуникациялық инфрақұрылымның маңызды объектілері.  \* Ақпараттық қауіпсіздік оқиғаларының мониторингі-ақпараттық қауіпсіздік оқиғаларын анықтау және сәйкестендіру мақсатында ақпараттандыру объектісін тұрақты бақылау.  3. Сатып алынатын қызметтердің мақсаттары  Сатып алынатын қызметтердің мақсаттары:  1. Үшінші тұлғалардан ақпараттық қауіпсіздіктің жедел орталығының қызметін сатып алу және ақпараттық қауіпсіздікті қамтамасыз ету мониторингі жүйелерін ақпараттық қауіпсіздікті ұлттық үйлестіру орталығының ақпараттық қауіпсіздікті қамтамасыз ету мониторингі жүйесінің техникалық құралдарына қосуды қамтамасыз ету туралы "ақпараттандыру туралы" Заңның талаптарын орындау.  2. "Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптар"Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысына сәйкес келтіру.  3. АТ-инфрақұрылымының қорғалу деңгейін арттыру және АҚ инциденттерінің залалын болдырмау үшін жағдайлар жасау.  4. ОСБ қызметтерінің құрамы  1. Ақ бұзылуына байланысты оқиғалардың мониторингі және Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысының 38-тармағына сәйкес мониторинг нәтижелерін талдау.  2. Осалдықтар мониторингі және Тапсырыс берушінің ақпараттандыру объектілерінің АҚ мониторингі нәтижелерін талдау.  3. Келесі ұрпақтың шабуылын анықтау жүйесін енгізу.  5. Қызметтерге қойылатын талаптар  Орындаушы "Ақпараттандыру туралы" ҚР Заңының 7-2, 7-3-баптарына сәйкес ОССБ қызметін көрсетеді және мәлімделген талаптарды орындауға байланысты барлық міндеттемелерді өзіне қабылдайды.  1. Қызмет көрсету кезеңі: шартқа қол қойылған күннен бастап 31.12.2025 дейін.  2. Платформаның келесі параметрлермен жұмыс істеуін қамтамасыз ету:  o платформаға қызмет көрсету мерзімі-24/7/365;  o бір айдағы технологиялық терезелер саны-1 - ден аспайды;  o тоқтап қалу туралы хабарлама-60 минуттан аспайды;  o технологиялық терезенің максималды ұзақтығы-6 сағаттан аспайды;  o технологиялық терезе туралы хабарлама-3 жұмыс күнінен аспайды.  3. Көрсетілетін қызметтердің техникалық және әкімшілік параметрлері:  o АҚ және желілік пакеттердің кіріс оқиғаларын өңдеу және талдау;  o секундына оқиғалардың өңделетін саны-2000 EPS дейін;  o көздер саны – шексіз;  O Орындаушы жұмысшылары үшін оқиғаларды өңдеу жүйесіне қол жеткізу-кемінде 10 пайдаланушы;  6. Қызметтердің сипаттамасы  6.1 ақ бұзылуына байланысты оқиғалардың мониторингі және Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысының 38-тармағына сәйкес мониторинг нәтижелерін талдау.  1. Тапсырыс беруші мен ОЦИБ платформасы арасында қорғалған байланыс арнасын орнату, желілік және қауіпсіздік параметрлерін орнату.  2. Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 28 наурыздағы №52/НҚ бұйрығының № 4 қосымшасымен айқындалған жазбалардың форматтары мен түрлеріне сәйкес қауіпсіздік оқиғаларын қалыптастыруға оқиғалар көздерін баптау.  3. Оқиғалардың типтік емес көздері үшін тапсырыс берушінің инфрақұрылымына оқиғаларды корреляциялау ережелерін әзірлеу және бейімдеу.  4. АҚ оқиғаларын бақылау және талдау 24/7.  5. АҚ-ның анықталған бұзушылықтары мен инциденттері туралы Тапсырыс берушіні АҚ-ның расталған инциденттері үшін оқшаулау жөніндегі ұсынымдармен хабардар ету.  6. Ақпараттандыру объектілерінің АҚ-обеспечения, АҚ-ның қауіп-қатерлері мен инциденттерін қамтамасыз ету үшін қажетті ақпаратпен алмасу бойынша ҰҚКҰК-мен өзара іс-қимыл жасау.  7. Заңнамалық талаптармен айқындалған кезең ішінде қауіпсіздік оқиғаларын жинауды, шоғырландыруды және сақтауды ұйымдастыру (3 ай. - жедел қолжетімділік, 3 жыл – мұрағаттық) Тапсырыс беруші жағында.  8. Тапсырыс берушінің өтініштерін тәулік бойы қабылдау және тіркеу.  9. Тапсырыс беруші мониторингке жататын көздердің тізімін айқындайды, ол екі тараптың қолы қойылған құжатпен бекітіледі  6.2 осалдықтар мониторингі және мониторинг нәтижелерін талдау  1. Қауіпсіздік сканерінің тұтынушы жағында орналастыру және орнату.  2. Тапсырыс берушімен келісілген көздер тізімінің осалдығына Желіні сканерлеу.  3. Сканерлеу нәтижелері бойынша мәліметтерді талдау және бағалау, осалдықтарды жіктеу, жою жөніндегі ұсынымдар, анықталған осалдықтар және оларды жою шаралары туралы есеп.  4. Есепті Тапсырыс берушіге жолдау.  5. Тапсырыс берушінің өтініштерін тәулік бойы қабылдау және тіркеу  6.3 келесі ұрпақтың интрузияны анықтау жүйесін бақылау  1. Келесі ұрпақтың интрузияны анықтау жүйесін орналастыру және конфигурациялау.  2. Қосылған көздер мен Тапсырыс берушінің инфрақұрылым желісі бойынша деректерді ұсынғаннан кейін бірегей тұзақтар жасау.  3. Келесі ұрпақтың интрузияны анықтау жүйесін бақылау.  4. Жүйе аймағында келесі ұрпақтың енуін анықтау бойынша анықталған инциденттер бойынша мәліметтерді талдау және бағалау  5. Тапсырыс берушінің талабы бойынша анықтау бойынша есептің бағыттары  6. Тапсырыс берушінің өтініштерін тәулік бойы қабылдау және тіркеу  7. Мониторинг тобын ұйымдастыруға қойылатын талаптар  1. Үздіксіз мониторинг: Қазақстан Республикасының ақпараттық-коммуникациялық технологиялары және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарға, Үкіметтің 2016 жылғы 20 желтоқсандағы № 832 қаулысына сәйкес ақпараттық қауіпсіздіктің тұрақты мониторингін ұйымдастыру міндетті болып табылады. Мониторингтік топ ақпараттық-коммуникациялық жүйелердің қауіпсіздігін басқару жөніндегі талаптарға енгізілген ақпараттық қауіпсіздік оқиғаларын бақылауды қамтамасыз ету үшін тәулік бойы (24/7) жұмыс істеуі тиіс.  2. Қызметкерлер саны: мониторинг тобы ҚР Еңбек кодексіне сәйкес жұмыс уақытының нормаларын сақтай отырып, үздіксіз функцияларды орындау үшін жеткілікті қызметкерлермен тәулік бойы (24/7) жұмыс істеуі тиіс.  3. Орындаушының аумақтық қатысуына қойылатын талап:  Орындаушының инциденттерге жедел ден қоюды қамтамасыз ету үшін Қазақстанның мынадай өңірлерінде өкілдіктері болуға тиіс:  Алматы қ., Астана қ., Ақтау қ., Ақтөбе қ., Атырау қ., Жезқазған қ., Қарағанды қ., Көкшетау қ., Қостанай қ., Қызылорда қ., Павлодар қ., Петропавл қ., Семей қ., Талдықорған қ., Тараз қ., Орал қ., Өскемен қ., Шымкент қ. Түркістан.  Жедел ден қою-Орындаушы оқиға расталған сәттен бастап 1 сағат ішінде Тапсырыс берушінің өңірлік бөлімшелеріне мамандардың келу уақытын қамтамасыз етуге тиіс.  Штаттық техникалық қолдау - әр өңірде сервистік жұмыстарды орындау үшін білімі мен құзыреті бар кемінде бір маман болуы тиіс.  Өкілдіктердің бар екендігін растау – конкурстық өтінімнің құрамында Орындаушы:  Мекенжайлары мен байланыс деректері бар Орындаушы өкілдіктерінің тізімі.  8. Ақпаратты қорғау жүйелеріне қойылатын талаптар  8.1 келесі ұрпақтың шабуылын анықтау жүйесіне қойылатын талап  1. Ұсынылған шешім соңғы пайдаланушы желісінің қолданыстағы топологиясын қайта құруды қажет етпестен орналастырылуы керек.  2. Ұсынылған шешім кем дегенде келесі модульдерді қамтуы керек:  a. орталық басқару түйіні,  b. тұзақ түйіні (жемді бастайтын),  c. соңғы құрылғылардағы Агент(Жем үгінділері).  3. Ұсынылған шешім Linux және Microsoft Windows операциялық жүйелері бар нақты желілік хосттарға пассивті жалған деректерді (үгінділер, жемдер) орналастыра алуы керек.  4. Ұсынылған шешім жүйенің компоненттерін қайта орнатуды қажет етпестен масштабталуы керек.  5. Ұсынылған шешім басқару операцияларын қолдау үшін арнайы функционалды данасы бар тұзақ (Жем) түйіндерінің көптеген даналары бар архитектураны қолдауы керек.  6. Ұсынылған шешім симуляциялық тұзақтарды (жемдерді) әртүрлі желілік сегменттерге орналастыру мүмкіндігіне ие болуы керек.  7. Ұсынылған шешім IP-трафик ағыны туралы кез келген ақпаратты (мысалы, желілік IP-трафиктің, NetFlow, sFlow, jFlow және т.б. шикі көшірмелері) кіріс ретінде пайдаланусыз жұмыс істеуі керек.  Басқаруға қойылатын талаптар:  8. Ұсынылған шешім интуитивті интерфейске ие болуы керек және оған техникалық қызмет көрсету мен қолдаудың айтарлықтай шығындарын қажет етпейді.  9. Ұсынылған шешім мультитенантты қолдауы керек, яғни бір консольде басқарылатын оқшауланған ортаны құру мүмкіндігі.  10. Бұл жағдайда жеке тенанттардың әкімшілері басқару консоліндегі олар үшін конфигурацияланған желі сегментіне ғана қол жеткізе алады, ал бас әкімші барлық есептік жазбаларға қол жеткізе алады.  11. Ұсынылған шешім жүйелік әкімшілерге құқықтар беру үшін RBAC (Role-Based Access Control, рөлдік қатынасты басқару) қолдауы керек.  12. Ұсынылған Шешім Басқару модуліндегі барлық әрекеттерге егжей-тегжейлі аудит жүргізуі керек. Параметрлерге өзгертулер енгізілген кезде, Аудит журналы өзгертілетін параметрлердің бастапқы және соңғы мәндерін нақты жазуы керек.  13. Ұсынылған шешім мультифакторлық аутентификацияны (MFA) қолдауы керек. Уақытпен байланысты бір реттік құпия сөз алгоритмін (TOTP) қолдау қажет.  14. Ұсынылған шешім жеткізушіні қолдау қызметі техникалық ақауларды дербес жою үшін журнал мұрағатын құра алуы керек.  Функционалдық талаптар:  15. Әрбір тұзақ (Жем) өзіндік сипаттамалар жиынтығымен (MAC мекен-жайы, IP мекен-жайы, Хост атауы, имитацияланған қызметтер мен параметрлер) ерекше болуы керек.  16. Тұзақтар IP-ге негізделген масштабтау опциясын пайдаланбауы керек, мұнда әр тұзақтың бірнеше IP-мекен-жайы болады, бұл инфрақұрылымдағы шабуылдаушыларға ұқсас тұзақтарды табуды едәуір жеңілдетеді.  17. Ұсынылған шешім мезгіл-мезгіл тұзақтар жасай алуы керек:  a. сыртқы веб-ресурстарға қосылу,  b. DNS, mDNS, LLMNR және NetBIOS арқылы хост атаулары мен домендік атауларға рұқсат беру,  c.SMB протоколы арқылы файл ресурстарының тізімін сұраңыз.  18. Ұсынылған шешім өндірістік ортадағы желінің нақты соңғы түйіндерінде жалған деректерді (breadcrumbs) құруға және таратуға мүмкіндік беруі керек.  19. Жалған деректер түрлері кем дегенде мыналарды қамтуы керек:  a. автолог үшін сақталған деректер,  b. имитацияланған деректер көздеріне қосылу профильдері,  c. желілік ресурстар,  d. сақталған RDP және SSH сеанстары,  e. имитацияланған мәліметтер базасына арналған есептік жазбалары бар конфигурациялық файлдар және т. б.  20. Ұсынылған шешім Жұмыс станцияларының хосттарында жалған кэштелген деректерді таратуға және құруға арналған құралдарды қамтуы керек.  21. Ұсынылған шешім желілік шабуылдарды анықтауы керек (brute force типті шабуылдарды анықтау, Имитациялық қызметтерге қосылу әрекеттері) және қауіптің түрі мен принципіне қарамастан олардың сыни тұрғыдан жіктелуі керек. Анықтау және жіктеу шифрланбаған және шифрланған трафикке қолданылуы керек.  22. Ұсынылған шешім тұзаққа қосылу тарихын және шабуылдаушының тұзақпен манипуляциялау тарихын көрсетуі керек:  а. бұзылған хосттың IP мекенжайын көрсете отырып,  b. бұзылған тіркелгі деректері,  c.өзара әрекеттесу хаттамалары/порттары.  23. Ұсынылған шешімде жүйенің, оқиғалардың және т. б. статистикасын көрсететін кіріктірілген графикалық панельдер болуы керек.  24. Ұсынылған шешім MITM типті шабуылдарды (ортадағы адам) анықтауы керек, соның ішінде:  a. ARP spoofing,  b. NBT / llmnr / mdns улануы,  c. HTTPS сұрауларын ұстау.  25. Ұсынылған шешім толығымен автоматты режимде тұзақтар жасай алуы керек.  26. Ұсынылған шешім кем дегенде тұзақ түрлерінің келесі тізімін қамтуы керек:  a. Microsoft RDP сервері,  b. Microsoft SMB файл сервері,  c. MS RPC қосылу әрекеттерін анықтауға арналған Microsoft MS RPC тұзағы,  d. Linux ОЖ бар серверлер,  e. QRadar веб-пайдаланушы интерфейсі,  f. VMware ESX веб-интерфейсі,  g. Fortinet веб-интерфейсі,  h. Microsoft Outlook Web Access веб-интерфейсі,  i. SCADA/HMI/PLC,  j. DNS сервері,  k. MySQL сервері,  l. PostgreSQL сервері,  m. FTP файл сервері,  n. Samba файл сервері,  o. Modbus TCP сервері,  p. MQTT брокері.  27. Ұсынылған шешім клиенттің желісінде қолданылатын кез-келген веб-сайт/веб-қызмет негізінде желілік тұзақтарды құра алуы керек. Бұл тұзақтарда веб-қызметтердің белгілі осалдықтары болуы керек (OWASP TOP 10).  28. Веб-тұзақтарда келесі конфигурация параметрлері болуы керек:  a. әр түрлі веб-серверлерді имитациялауға арналған сервер тақырыбы,  b. тұзаққа DoS шабуылдарының алдын алу үшін жылдамдықты шектеу,  c. жарамды HTTP әдістері,  d. мұндай тұзақтардағы реттелетін жолдар мен файлдар, соның ішінде жауап,  e. ерікті HTTP тақырыптарын қосу,  F. TLS-веб-тұзаққа арналған сертификат.  29. Ұсынылған шешім Жем файлдарын регенерациялауға, соның ішінде осы Жем файлдарының мазмұнының дәйектілігі мен сенімділігін қамтамасыз ету үшін желілік жемдерді қайта құруға мүмкіндік беруі керек.  30. OT тұзақтары Rockwell Automation PLC компаниясының Siemens және Allen-Bradley веб-интерфейстеріне еліктеуі керек.  31. OT тұзақтары s7comm және Modbus TCP протоколдарын қолдауы керек.  32. Ұсынылған шешім жүйенің операторларын қарау және өңдеу үшін көптеген Оқиғалармен шамадан тыс жүктемеу үшін анықталған шабуылға байланысты оқиғаларды бір хабарламаға дәл жіктеп, біріктіруі керек.  33. Ұсынылған шешім жүйеде бар негізгі түрлерге негізделген желілік тұзақтардың жеке түрлерін жасауға мүмкіндік беруі керек. Тұзақтың жаңа түрін жасағаннан кейін, пайдаланушы қосымша манипуляциясыз бірден таңдалған түрдегі бірнеше тұзақты автоматты түрде жасай алуы керек. Тұзақтардың жаңа түрлерінің конфигурациясы қарапайым және стандартталған мәтін түрінде болуы керек (YAML немесе JSON).  34. Ұсынылған шешімде әрбір өңделген хабарламаның күйін көрсететін irms (қауіпсіздік инциденттерін басқару жүйесі) функционалдығы болуы керек.  35. Өзара әрекеттесу деңгейі жоғары тұзақтар кем дегенде сканерлеуге жауап беру, тіркелгі деректерін сұрау және графикалық және/немесе мәтіндік интерфейсті көрсету деңгейінде интерактивтілікті қамтамасыз етуі керек. Әрбір тұзақ бірегей болуы керек, оның IP-мекен-жайы бар, IP-alias және full os технологиясын қолданбай.  36. Ұсынылған шешім қолтаңбаларды пайдаланбай киберқауіптерді анықтау әдісін қолдануы керек.  37. Ұсынылған шешім желілік активтердің бір-бірімен өзара әрекеттесуін құру және визуализациялау мүмкіндігіне ие болуы керек.  38. Ұсынылған шешім қауіпсіздік туралы хабарламалармен байланысты желілік трафиктің қоқысын құруы керек. Желілік трафиктің қоқысы PCAP форматында болуы керек.  39. Бағдарламалық платформа заңды Қызметтерді қосу мүмкіндігіне ие болуы керек  8.2 осалдықтарды басқаруға қойылатын талаптар  1. Жүйе кем дегенде 1024 желі активтері үшін осалдықтарды басқару процесін қамтамасыз етуі керек.  2. Жүйе активтердің шексіз саны үшін активтерді түгендеу мақсатында сканерлеуді қамтамасыз етуі керек.  3. Осалдықтар туралы ақпарат қосымша қосымшаларды немесе кеңейтімдерді орнатпай-ақ жүйенің Siem интерфейсі арқылы қол жетімді болуы керек.  4. Осалдықтарды басқару жүйесі деректерді пайдалануы керек SIEM осалдықтарды түзету процесінің басымдылығын қамтамасыз ету үшін жүйелер мен конфигурацияны басқару жүйелері.  5. Табылған осалдықтар туралы деректер оқиғаларды анықтау үшін Siem корреляциялық ережелерінің іске қосылуына автоматты түрде әсер етуі керек.  6. Әрбір осалдық актив иесіне автоматты түрде бекітілуі керек және табылған осалдықты түзету үшін уақыт аралығын орнату және оны автоматты түрде жою мүмкіндігі берілуі керек. Актив иесіне: электрондық пошта немесе жүйенің Siem интерфейсі арқылы хабарлау керек.  7. Жүйе сканерлеу процесін автоматты түрде іске қосуға мүмкіндік беруі керек: кез-келген ақпараттық қауіпсіздік оқиғалары/инциденті, желідегі жаңа активті келесі мәліметтер негізінде анықтау: оқиғалар журналдары (logs), NetFlow деректері, jFlow деректері, sflow деректері, ipfix деректері, активтің ОЖ конфигурациясын өзгерту, немесе деңгейінде жаңа есептік жазба құру Актив ОЖ.  8. Жүйе кесте бойынша инфрақұрылымды ішкі және сыртқы сканерлеудің функционалдығын қамтамасыз етуі керек.  9. Сканерлеу саясаттары сканерлеу түріне (Web Scan, Patch Scan, Discovery Scan, Database Scan, Full Scan), сондай-ақ жаңа сканерлеу саясаттарын немесе реттелетін үлгілерді жасау мүмкіндігіне сәйкес орнатылуы керек.  10. Сканерлеу түрін анықтау керек: сканерлеу ХАТТАМАСЫ, сканерлеу порттарының ауқымы және сканерлеу активтерінің топтары.  11. Осалдықтарды басқару жүйесі үшінші тарап қолданбаларын, дерекқорларды, қосымша интерфейстерді, терезелерді немесе басқа виртуалды құрылғыларды: IBM Guardium, AXIS Scanner, Beyond Security avds, digital Defence inc.іске қосуды және пайдалануды қажет етпей, веб-интерфейс арқылы инфрақұрылымдық интеграция арқылы келесі сканерлер үшін кесте бойынша сканерлеуді іске қосу және ақпаратты автоматты түрде алу параметрлерін орнатуға мүмкіндік беруі керек. AVS, eEye REM Scanner, FoundScan Scanner, SiteProtector, BigFix, Juniper NSM Profiler, McAfee VM, Microsoft SCCM, nCircle IP360 Scanner, Nessus Scanner, NMap Scanner, Outpost24 Vulnerability Scanner, Positive Technologies MaxPatrol, Qualys Detection Scanner, Qualys Scanner, Rapid7 NexPose Scanner, Saint Scanner, SecureScout Scanner, Tenable Security Center.  12. Веб-қосымшаларды сканерлеу кезінде Open Web Application Security Project TOP 10 таксономияларына сәйкес осалдықтарды анықтауға мүмкіндік беретін эвристикалық талдау әдістерін қолданыңыз.  13. Бірыңғай Siem интерфейсі арқылы пайдаланушы келесі мүмкіндіктерге ие болуы керек:  14. Құрылғыларды, веб-қосымшаларды, ішкі желілерді және сыртқы периметрді сканерлеуді іске қосыңыз.  15. Құрылғыларға, веб-қосымшаларға, ішкі желілерге және сыртқы периметрге арналған икемді сканерлеу сценарийлерін теңшеңіз, мысалы: әр 3 күн сайын, сағат 13.00-де сканерлеу.  16. "Сканерлеу тереңдігін" теңшеңіз, мысалы - әкімші өкілеттіктерін пайдалану немесе онсыз.  8.3 осалдық сканеріне қойылатын талаптар  Жалпы талаптар  1. Осалдық сканері бір платформада активтер мен осалдықтардың толық көрінуіне ие болуы керек.  2. Желідегі барлық активтерді, соның ішінде физикалық құрылғыларды, виртуалды машиналарды, бұлттық ресурстарды, контейнерлерді және IoT құрылғыларын анықтау мүмкіндігі болуы керек.  3. Осалдық сканерінде желідегі жаңа активтерді автоматты түрде анықтайтын және оларды түгендеуге қосатын функционалдылық болуы керек.  4. Платформа конфигурацияны басқару жүйелерімен (CMDB), SIEM және ITSM интеграциясын қолдауы керек.  5. Сканерде өзектілікті қамтамасыз ету және өзекті технологияларды пайдалану үшін осалдықтар базасының тұрақты жаңартулары болуы керек.  6. Анықтаудан бастап жоюға дейінгі осалдықтардың өмірлік циклін басқару үшін түпкілікті интеграцияны қолдау мүмкіндігі.  7. Кесте бойынша да, сұраныс бойынша да желіні шексіз түгендеу сканерлеу мүмкіндігі  8. Агенттердің көмегімен де, агентсіз режимде де осалдықтарды сканерлеу мүмкіндігі  9. Кесте бойынша да, талап бойынша да осалдықтар бойынша Желіні сканерлеу мүмкіндігі  10. Осалдықтар базасына қол жетімділікті қамтамасыз ету, осалдықтарды сипаттау, сондай-ақ оларды жою бойынша ұсыныстар  11. Платформаның деректер орталығынан периметрдің осалдығын сканерлеу мүмкіндігі  12. Агентсіз сканерлеу үшін сканерлеу профильдерін орнату мүмкіндігі болуы керек (кем дегенде):  1. Сканерлеу қарқындылығы  2. Белгілі бір порттарды сканерлеу  3. Есептік жазбаны пайдалану  4. Қатыгез шоттар  5. Сканерлеу осалдықтарын таңдау  13. Инфрақұрылымды қайта сканерлеусіз (Тарихи деректер негізінде)жаңа осалдықтарға инфрақұрылымға талдау жүргізу мүмкіндігі  14. Ішкі кәсіпорын желісін агентсіз сканерлеу үшін қорғалған виртуалды машинаны(ларды)пайдалану керек  15. Жабдықта стандартты парольдердің болуын тексеру мүмкіндігі  16. Кем дегенде келесі платформаларда аутентификация мүмкіндігі: Windows, Unix ,acacle ,acacle 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 Сервер ,acacle WebLogic Server, Docker  17. Сканерлеу үшін тіркелгі деректерін алу үшін келесі Password Vaults-пен біріктіру мүмкіндігі: CyberArk Pim Suite, CyberArk AIM, Thycotic Secret Server, Quest Vault, CA Access Control, Hitachi ID PAM, Lieberman ERPM, BeyondTrust PBPS, Hashicorp Vault  18. Бір құрылғыда бірнеше жүйе болған кезде (Операциялық жүйе, дерекқор, Web сервер және т. б.) – шешім бір сканерлеу шеңберінде қажетті есептік жазбалары бар барлық жүйелерді бағалауға мүмкіндік беруі керек (технологияларға байланысты қажетті есептік жазбаларды автоматты түрде таңдау)  19. Платформада сканерлеу процесі есеп беру процесінен бөлінуі керек: барлық сканерлеу осалдықтар бойынша орталық базаны толтыруы керек  20. Жүйе инфрақұрылымдағы осалдық күйін және инфрақұрылымда болу уақытын бақылауы керек  21. Жүйе инфрақұрылымдағы осалдықтар үшін кем дегенде келесі мәртебелерді қамтамасыз етуі керек:  1. жаңа осалдық (1 рет анықталды)  2. белгілі осалдық (2 + рет анықталған)  3. түзетілген осалдық (жаңа/танымал болды, бірақ жүйе оны инфрақұрылымда анықтауды тоқтатты)  4. қайта ашылған осалдық (түзетілді, бірақ инфрақұрылымда қайта пайда болды)  22. Платформа 24/7/365 сыни ресурстарды үздіксіз сканерлеуге мүмкіндік беруі керек  23. Модуль осалдықтарды тексеруді OVAL форматында немесе сипатталған басқа форматта қосуға мүмкіндік беруі керек. Қолтаңбаларды сипаттау форматы құжатталуы керек.  Қауіпсіздікті талдау жүйесінің есептілігіне қойылатын талаптар  1. Пайдаланушы алдын ала орнатқан ережелер негізінде құрылғыларды автоматты түрде динамикалық таңбалау мүмкіндігі:  a. IP ішкі желісіне тиесілі  b. NetBIOS және FQDN атауын талдауға негізделген  c. Операциялық жүйе негізінде  d. ашық порттар/қызметтер бойынша  e. нақты осалдықтың болуы бойынша  f. сканерлеу мерзімдері негізінде  2. Таңбалау тұқым қуалайтын ағаш тәрізді маркер құрылымдарын қолдауы керек  3. Кесте бойынша да, талап бойынша да есептерді қалыптастыру мүмкіндігі  4. Компания талаптарына сәйкес есептерді теңшеу мүмкіндігі  5. Есепте келесі ақпарат болуы мүмкін / болуы керек:  а. вендор шкаласы бойынша және CVSS бойынша осалдықтың атауы және оның сыни деңгейі  b. осал жүйелердің немесе сервистердің тізбесі  c. осалдық күйі (жаңа / белсенді / түзетілген)  d. осалдықты жою бойынша ұсыныстар немесе егер бар болса, патч сілтемесі  e. осалдыққа басымдық берудің қосымша критерийлері: эксплуатацияның, зиянды кодтың және т.б. болуы.  6. Платформа белгілі бір осалдық түрі бойынша есептерді сүзу мүмкіндігін қамтамасыз етуі керек:  а. патчтың болуы негізінде  b. нақты эксплуатациялық пакеттерде эксплуатацияның болуы негізінде  c. осалдық үшін зиянды кодтың болуы  d. cvss рейтингіне (CVSSv2, CVSSv3)  e. cvss шабуыл векторына  F. сатушыға және өнімге  g. сыни осалдық  h. CVE ID  i.және т. б.  7. Есеп беру жүйесі билеттерді құруға және оларды белгілі бір адамдарға тағайындауға мүмкіндік беруі керек  8. Басшылыққа арналған есептер. Сканерлеу нәтижелері және осалдықтарды анықтау немесе жою бойынша графикалық трендтерді құра отырып ақпаратты қысқаша ұсыну  9. Осалдықтар бойынша емес, жаңартулар бойынша IT мамандарына арналған есептер  10. Жүйелерді агентсіз сканерлеу кезінде аутентификацияның сәтті өтуі туралы есептер  11. Жүйе анықталған осалдықтар бойынша талдауды және осалдықтарды жоюға басымдық беру құралдарын ұсынуы керек  12. Жүйе келесі деректер негізінде хосттарды, осалдықтарды және қажетті жаңартуларды көрсете отырып, қауіптерге басымдық беру үшін динамикалық есепті қалыптастыруға мүмкіндік беруі керек:  a. инфрақұрылымда осалдықтың болу уақыты  b. осалдықты жариялау уақыты  c. келесі шабуыл векторларының болуы:  i. іске қосылған қызмет  ii. Жүйенің белсенді ядросы  iii. Конфигурацияны өзгерту арқылы осалдықты жою  iv. Қашықтан сканерлеу арқылы осалдықты анықтау  v. жалпыға ортақ IP мекенжайы бар құрылғы  d. мынадай қауіп-қатер индикаторларының болуы:  i. осалдықты пайдаланудың оңай мүмкіндігі  ii. Осалдық үшін патчтың болмауы  iii. Осалдықты пайдалану кезінде деректердің жоғалу қаупі  iv. Жария эксплуатацияның болуы  v. осалдық үшін зиянды кодтың болуы  vi. Осалдықты пайдалану кезінде қызмет көрсетуден бас тарту қаупі (DoS)  vii. Осалдық шабуылдарда белсенді қолданылады  viii. Жария эксплуатациялық пакеттерде эксплуатацияның болуы  ix. Инфрақұрылым ішінде жылдам таралу қаупі  x. осалдық артықшылықтарды арттыру үшін қолданылады  xi. Осалдық ерікті кодты орындау үшін қолданылады  13. Жүйе нақты уақыт режимінде компания ресурстарының қорғалу мәртебесін көрсетуі керек (алдын ала орнатылған дешбордтар арқылы)  14. Жүйе пайдаланушыларға өздерінің dashboard виджеттерін жасауға мүмкіндік беруі керек  15. Жүйе дашбордтар мен виджеттерді түсіру мүмкіндігін қамтамасыз етуі керек  16. Есеп беру жүйесі барлық талданған ресурстар бойынша түпкілікті іздеу мүмкіндігін қамтамасыз етуі тиіс  17. Есептерден кейіннен алып тастай отырып, осалдықты таңбалау мүмкіндігі (жалған іске қосылған жағдайда)  Функционалдық талаптар  1. Платформа пассивті мониторинг пен агенттік тәсілді қолдана отырып, нақты уақыт режимінде активтерді түгендеуді қолдауы керек.  2. Жүйенің функционалдығы болуы керек келесі факторларға негізделген осалдықтарға автоматты түрде басымдық беру:  A. тәуекел деңгейі (cvss v2/v3).  B. Эксплуатациялардың болуы және танымалдығы.  C. активтердің бизнес-сыни контексті.  D. бизнеске ықтимал әсер ету.  3. Автоматтандырылған процестерді (Remediation Workflow) пайдалана отырып, осалдықтарды түзетуді қадағалау мүмкіндігі іске асырылды.  4. Қауіпсіздік туралы есептер осалдықтарды басқару тиімділігін бағалау үшін көрсеткіштерді, аналитиканы және болжамды үлгілерді қамтуы керек.  5. Кесте бойынша немесе сұраныс бойынша сыртқы және ішкі инфрақұрылымды сканерлеуді қолдау.  6. Әр активте бағдарламалық жасақтама лицензияларын анықтау және басқару мүмкіндігі.  7. Активтерді мақсаты, түрі және іскерлік маңыздылығы бойынша автоматты жіктеу функционалы.  8. Патчты басқару процестеріне интеграцияланған осалдықтарды түзетуді автоматтандыру сценарийлерін құру функциясы (Patch Management).  9. Қауіпсіздік стандарттарына негізделген конфигурациялық осалдықтарды анықтау функциясы.  10. Пайдаланылатын кітапханаларға және бағдарламалық жасақтаманың үшінші тарап компоненттеріне осалдықтың тәуелділігін талдау функциясы.  11. Қорғаныс процестері шеңберінде зиянды бағдарламалар мен қауіптерді анықтау функционалы.  12. Жүйе эксплуатациялық кодтың жетілуі, нақты ортадағы осалдықты белсенді пайдалану, активтің сыни сипаты және оның орналасқан жері сияқты бірнеше факторларға негізделген нақты тәуекел деңгейін автоматты түрде бағалау үшін қауіптер мен эксплуатациялар туралы толық ақпаратты пайдалануы керек.  13. Жүйе өзінің логикасы мен қауіп-қатер қолтаңбаларын қолдана отырып, тапсырыс бойынша әзірлемелер мен бағдарламалық жасақтамадағы осалдықтарды анықтауға, басқаруға және жоюға мүмкіндік беруі керек.  Техникалық талаптар  1. Барлық негізгі протоколдар бойынша сканерлеуді қолдау (TCP, UDP, HTTP, HTTPS және т.б.).  2. Сканерлеу тереңдігін, соның ішінде Әкімші өкілеттіктерімен немесе онсыз сканерлеуді орнату.  3. Пайдаланушы саясаты мен сканерлеу үлгілерін жасау мүмкіндігі.  4. Веб-қосымшалардағы осалдықтарды анықтау үшін эвристикалық талдау әдістерін қолдану.  5. Активтердің күйін, осалдықтарын және түзетулердің барысын қоса алғанда, жиынтық бақылау тақталарында деректерді визуализациялау.  6. Тарихи деректер негізінде трендтерді талдау және тәуекелдерді болжау.  7. Осалдықтың активтерге және желінің ішкі желілеріне әсерін автоматты түрде бағалау.  8. Осалдықтарды түзету үшін қажетті уақыт пен ресурстарды болжау.  9. Активтерді тұрақты бақылау үшін агенттік тәсілдің жұмысын қолдау.  Пайдаланушы интерфейсі  1. Бір басқару терезесі арқылы негізгі мүмкіндіктерге қол жеткізе алатын интуитивті интерфейс.  2. Икемді сканерлеу сценарийлерін орнату(мысалы, берілген уақытта үш күн сайын талдау).  3. Электрондық пошта, мессенджерлер және басқа да ескерту жүйелері арқылы табылған осалдықтар туралы хабарламалар.  4. Сүзгілермен, реттелетін өрістермен және визуализациямен теңшелген есептерді жасау мүмкіндігі.  5. Есептерді кесте бойынша жауапты тұлғаларға автоматты түрде жіберу.  6. Жүйенің конфигурациясындағы өзгерістерден кейін сканерлеуді белсендіруді қоса, анықталған осалдықтарға жауап беру сценарийлерін орнату.  Қауіпсіздік және сәйкестік  1. ISO/IEC 27001 қоса алғанда, халықаралық қауіпсіздік стандарттарына сәйкестігі.  2. Тасымалдау және сақтау кезінде деректерді шифрлауды қолдау.  3. Барлық операцияларды тексеру және тіркеу функциялары жүзеге асырылады.  4. Теңшелетін құралдармен интеграциялау және осалдықтарды басқаруды автоматтандыру үшін API қол жетімділігі.  Өнімділік және масштабтау  1. Ірі желілерде жұмыс істеуді қолдау.  2. Желідегі жүктемені азайту үшін таратылған сканерлеу мүмкіндігі.  3. Желінің өнімділігіне минималды әсер ететін жоғары сканерлеу жылдамдығы.  Қолдау және қызмет көрсету  1. Жеткізушіден тәулік бойы техникалық қолдау.  2. Пайдаланушы нұсқаулығын, техникалық сипаттамаларды және оқу материалдарын қоса алғанда, егжей-тегжейлі құжаттамаға қол жеткізу.  3. Бағдарламалық жасақтама мен осалдық дерекқорын автоматты түрде жаңарту.  4. Пайдаланушы форумдары мен оқу ресурстарын қолдау (вебинарлар, білім базалары).  9. Орындаушыға қойылатын талаптар  9.1 Орындаушы аккредиттелген органдар берген ISO/IEC 27001 стандарттарына сәйкестік сертификаттарын ұсынуы керек, бұл компанияның деректер қауіпсіздігін басқару саласындағы құзыреттілігін растайды.  9.2 Орындаушы орындалған жұмыс туралы ай сайынғы есептерді ұсынуға міндетті, онда анықталған инциденттер, оқиғаларды өңдеу статистикасы және қауіпсіздік деңгейін арттыру бойынша ұсынылған шаралар жазылуы тиіс. Сондай-ақ қызметкердің аты-жөнін, ауысым күні мен уақытын қамтитын қызметкерлердің ауысымдық кестесі қоса беріледі.  9.3 Орындаушы Тапсырыс беруші ұсынған ақпаратты қорғау құралдарын пайдалана отырып, ақпараттық қауіпсіздік оқиғаларының мониторингін және инциденттерін талдауды жүзеге асырады.  9.4 Орындаушы Тапсырыс берушімен бірлесіп Тапсырыс беруші ұсынған ақпаратты қорғау құралдарына қорғалған VPN-туннельді ұйымдастыруды қамтамасыз етеді.  10. АҚ инциденттерін тергеу үшін Деректер беру  Ақ инцидентін өңдеу кезінде ақ инцидентін тергеуге жауапты орындаушының қызметкері тапсырыс берушіден инцидент бойынша ақпарат жинайды, ол мынадай деректерді береді:  10.1 оқиға тіркелген филиал, аймақ.  10.2 оқиғаның пайда болу уақыты.  10.3 IC, IP мекенжайлары, MAC мекенжайлары, FQDN-оқиғаға қатысты хост атаулары.  10.4 оқиғаға қатысты жүйелерді пайдалануға жауапты қызметкердің байланыс деректері (аты-жөні, телефоны, электрондық пошта мекенжайы).  10.5 оқиғаның сыни сипаты.  11. АҚ инциденттеріне тергеу жүргізу  Инцидент бойынша бастапқы ақпаратты жинағаннан кейін инцидентті тергеуге жауапты АҚ инцидент бойынша кеңейтілген ақпаратты жинауға кіріседі, оған мыналар кіреді:  11.1 инцидент фигуранттары туралы қосымша деректерді жинау (басқа ақпараттық, инфрақұрылымдық жүйелердегі, 1 айдан бастап алдыңғы кезеңдегі ақпаратты қорғау жүйелеріндегі фигуранттармен болған оқиғалар; қол жетімді қолжетімділік/рөлдер/артықшылықтар; бұрын тіркелген АҚ инциденттерінің болуы).  11.2 оқиғаға қатысушы жүйелер туралы қосымша деректерді жинау (тіркелген оқиғалар мен ақ инциденттері, автоматтандырылған сканерлеу, тексеру және аудит нәтижелері).  11.3 АҚ оқиғасына қатысты басқа қосымша ақпарат.  Бұл жұмыс Тапсырыс берушімен бірлесіп жүргізіледі. Тергеу сапасы Тапсырыс беруші ұсынатын деректерге байланысты.  11.4 жиналған ақпараттың нәтижелері бойынша АҚ инцидентіне тергеу жүргізіледі. Оқиғаны тергеу барысында Орындаушының қызметкері:  \* АҚ оқиғасының туындауына әкеп соққан оқиғалардың хронологиясы.  \* АҚ оқиғасының себептері.  \* Ақ оқиғасының жалғандығы немесе ақиқаты.  \* АҚ оқиғасының салдары.  11.5 АҚ инцидентін тергеу қорытындысы бойынша атқарылған жұмыс туралы есеп қалыптастырылады. Орындаушы оқиғаны талдаудан және қайнар көзі мен себептерін анықтаудан басқа, Болашақта ұқсас оқиғалардың пайда болу ықтималдығын болдырмауға немесе азайтуға мүмкіндік беретін техникалық ұсыныстар жиынтығын қалыптастырады.  11.6 Тапсырыс беруші өзіне берілген ақпаратты талдайды, берілген ұсынымдардың өз инфрақұрылымында қолданылуы туралы шешім қабылдайды және ұсынылған техникалық іс-шараларды жүргізеді.  11.7 ұсынылған алдын алу тетігін Орындаушы мен Тапсырыс беруші оқиға туындаған кезде қайта қолдану мүмкіндігіне талдайды және жүйенің бейінін сипаттайтын құжаттамада тіркеледі.  12. Жаңа көздерді ОЦИБ жүйесіне қосу  Тапсырыс беруші келесі ақпаратты ұсына отырып, ақ оқиғаларының қосымша көзін қосуға сұрау салуды бастайды:  12.1 көз түрі.  12.2 дереккөзден деректерді алу туралы ақпарат (IP мекенжайы, қол жеткізу деректері).  12.3 осы дереккөз шеңберінде бақылануы қажет оқиғаларды анықтау сценарийлерінің тізімі.  12.4 инциденттерді анықтау сценарийлеріндегі жүйені анықтау үшін қажет қосымша ақпарат.  12.5 Орындаушы Тапсырыс берушінің мамандарымен бірлесіп, мақсатты көзден қажетті оқиғаларды жинаудың техникалық мүмкіндігін бағалайды және қосылу механизмі мен тәсілін келіседі.  12.6 Орындаушы жұмыстарды орындау үшін берілген ақпараттың жеткіліктілігін бағалайды және жаңа көзді қосуды ескере отырып, оқиғаларды анықтау сценарийіне өзгерістер енгізеді.  12.7 Орындаушы мен Тапсырыс берушінің қызметкерлері АҚ оқиғаларын жинау жүйесінде және оны қосу үшін көзде қажетті параметрлерді орындайды.  12.8 қосылу және жұмысқа қабілеттілігін тексеру аяқталғаннан кейін Орындаушы Тапсырыс берушімен бірлесіп екі тараптың қолымен жасалған жұмыстар актісін ресімдейді  13. ОЦИБ жүйесінен көзді ажырату  Тапсырыс берушінің қызметкері келесі ақпаратты бере отырып, көзді өшіру туралы сұранысты бастайды:  13.1 көз түрі.  13.2 дереккөз идентификаторы (IP мекенжайы, қосымша).  13.3 Орындаушы инциденттерді анықтаудың қолданыстағы сценарийлеріне талдау жүргізеді және егер дереккөзді өшіру оларды өзгертуге немесе бақыланатын инциденттер тізімінен шығаруға әкеп соқтырған жағдайда Тапсырыс берушінің қызметкерлерін хабардар етеді.  13.4 қажет болған жағдайда Орындаушы мен Тапсырыс берушінің қызметкері АҚ оқиғаларын жинау жүйесіндегі және оны өшіру үшін көздегі оқиғалардың құрамын өзгерту бойынша жұмыстарды орындайды.  13.5 ажырату және жұмысқа қабілеттілігін тексеру аяқталғаннан кейін Орындаушы Тапсырыс берушімен бірлесіп екі тараптың қолымен жасалған жұмыстардың актісін ресімдейді  14. Инциденттерді анықтаудың жаңа ережелерін іске асыру  14.1 Тапсырыс беруші қажет болған жағдайда мынадай ақпаратты бере отырып, ақ инциденттерін анықтаудың жаңа ережесін (60-тан аспайтын) іске асыруға сұрау салуға бастамашылық жасайды:  \* Оқиғаның жалпы сипаттамасы және критерийлері.  \* Оқиғаны анықтауға арналған деректер көздерінің түрі.  \* Оқиғаның жоспарлы сыны.  14.2 Орындаушы ақ инциденттерінің туындау қатерлерінің сценарийін неғұрлым егжей-тегжейлі пысықтау үшін Тапсырыс берушінің мамандарын тарта отырып, ОСО жүйесінде Тапсырыс берушінің инфрақұрылымы шеңберінде ережені іске асырудың техникалық мүмкіндігін талдайды.  14.3 Орындаушы мен Тапсырыс берушінің қызметкерлері жаңа ереже бойынша оқиғаны анықтаудың қорытынды сценарийін келіседі, оның сыншылдығын және оқиға бойынша өзара іс-қимыл процесін айқындайды.  14.4 Орындаушы ОЦИБ жүйесінің параметрлерін жасай отырып, жаңа ережені іске асыру бойынша жұмыстарды орындайды.  14.5 баптау және жұмысқа қабілеттілігін тексеру аяқталғаннан кейін Орындаушы Тапсырыс берушімен бірлесіп екі тараптың қолдарымен жасалған жұмыстар актісін бекітеді.  Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметтердің құны айына ҚҚС-сыз 3 224 177,00 теңгеден аспайды |
| Шығарылған жылы | 2025 |
| Кепілдік мерзімі (айлармен) | 12 ай |
| Сатып алынатын тауардың талап етілетін функционалдық, техникалық, сапалық, пайдалану және өзге де сипаттамаларының сипаттамасы |  |
| Ілеспе қызметтер (қажет болған жағдайда көрсетіледі) (тауарларды монтаждау, баптау, оқыту, тексеру және сынау) | Жеткізуші серверлік жабдықта орнатуды (қашықтан) және конфигурациялауды орындауға міндетті. |
| Әлеуетті жеткізуші жеңімпаз деп анықталған және онымен мемлекеттік сатып алу туралы шарт жасалған жағдайда оған қойылатын шарттар (қажет болған жағдайда көрсетіледі) (Әлеуетті жеткізушіні көрсетілген мәліметтерді көрсетпегені немесе бермегені үшін қабылдамауға жол берілмейді) |  |

\* мәліметтер мемлекеттік сатып алу жоспарынан алынады (автоматты түрде көрсетіледі).

      Ескерту.

      1. Функционалдық, техникалық, сапалық, пайдаланушылық, өзге де сипаттамалар, ілеспе қызметтер бойынша әрбір талап және қосымша талаптар бөлек жолда көрсетіледі.

      2. Осы техникалық ерекшелікте әлеуетті жеткізушіге қойылатын біліктілік талаптарын белгілеуге жол берілмейді.

      3. Өзге құжаттарда техникалық ерекшеліктің талаптарын белгілеуге жол берілмейді.