«Universal Mobile Systems»
Mas'uliyati cheklangan jamiyati

Общество с ограниченной
ответственностью
«Universal Mobile Systems»

O'zbekiston, 100000
Toshkent shahri, Amir
Temur shoh ko'chasi, 24.
Tel: (+99897) 403 83 35
Faks: (+99871) 235 81 60,
e-mail: info@mobi.uz
www.mobi.uz

УТВЕРЖДАЮ
Директор по информационной безопасности
и режиму ООО «UMS»



_____Олматов Б.А.
«02» октября 2026г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на поставку, установку и запуск в эксплуатацию
Системы управления информацией и событиями безопасности (SIEM)
для нужд ООО «UNIVERSAL MOBILE SYSTEMS»

Ташкент – 2026

Оглавление:

1 Общие сведения 3
2 Основание для реализации проекта 3
3 Перечень работ, услуг и их объемы (количество), требуемые от Исполнителя 3
4 Место выполнения работ и оказания услуг 4
5 Технические требования к Системе 5
6 Требования к Исполнителю 13
7 Требования к безопасности выполнения работ и оказания услуг 14
8 Требования по передаче технических и иных документов по результатам выполненных работ и оказанных услуг 14
9 Требования к обучению персонала Заказчика 14
10 Гарантийные обязательства 15
11 Условия сервисной поддержки и техническое сопровождение 15
12 Требования к технической поддержке 16
13 Иные требования к работам, услугам и условиям их оказания 16
14 Используемые термины и сокращения 17
15 Перечень приложений 19

1 Общие сведения

В настоящем Техническом задании описаны требования к Системе управления информацией и событиями безопасности SIEM (далее - Система, ИС), достаточные для описания требований Заказчика к составу ПО, с целью объявления тендера и/или конкурса на приобретение ПО и услуг для реализации проекта в целом на условиях «под ключ».

Характеристика объекта информатизации представлена в Приложении №1.

1.1 Наименование выполняемых работ и оказываемых услуг

Полное наименование проекта: Система управления информацией и событиями безопасности SIEM (далее по тексту – Система).

Работы проводятся на инфраструктуре и площадке Заказчика.

В рамках данного Технического задания Исполнитель должен предоставить предложение на поставку ПО, установку, внедрение и запуск в эксплуатацию программного комплекса SIEM.

1.2 Цели использования выполняемых работ и оказываемых услуг

Основная цель проекта – это внедрение на инфраструктуре ООО «UMS» инструмента мониторинга и управления информацией о событиях информационной безопасности на инфраструктуре Компании.

Основные задачи, решаемые Системой:

- централизованный сбор и хранение событий безопасности;
- непрерывный мониторинг ИТ- и сетевой инфраструктуры;
- выявление инцидентов информационной безопасности;
- анализ и расследование инцидентов;
- формирование единой картины состояния ИБ;
- поддержка реагирования на инциденты;
- подготовка отчетов и аналитики;
- контроль соблюдения требований информационной безопасности.

Основное назначение Системы – централизованный сбор, анализ и корреляция событий информационной безопасности с целью своевременного выявления, расследования и реагирования на инциденты возникающие в компании ООО «UMS».

2 Основание для реализации проекта

Запланированный на 2026г. план развития Департамента безопасности и режима (утвержденный Бизнес план и Бюджет ООО «UMS» на 2026 год).

3 Перечень работ, услуг и их объемы (количество), требуемые от Исполнителя

Внедрение Системы SIEM должно проводиться совместно с ответственными лицами Заказчика, без нарушения работоспособности существующей ИТ-инфраструктуры Заказчика, с предварительным поверхностным обследованием имеющихся Веб-ресурсов и Веб-приложений. Все работы, требующие остановку каких-либо корпоративных систем должны быть предварительно согласованы с Заказчиком.

В рамках проекта Исполнителем должны быть выполнены следующие этапы работ:

- подготовительный этап;
- пуско-наладочные и интеграционные работы;
- обучение персонала Заказчика.

3.1 Подготовительный этап

Включает в себя взаимодействие с ответственным за Проект персоналом Заказчика и совместное обследование ИТ инфраструктуры Заказчика. На данном этапе сотрудники должны определить:

- наиболее важные детали топологии сети Заказчика;
- зоны ответственности Заказчика и Исполнителя в ходе развёртывания Системы;
- количество ИТ ресурсов, которые будет мониторить и защищать Система.

3.2 Пуско-наладочные и интеграционные работы

Во взаимодействии с ответственным за Проект персоналом Заказчика пуско-наладочные работы включают в себя:

- инсталляцию и конфигурацию программной части Системы;
- интеграцию в сетевую инфраструктуру Заказчика;
- активацию модулей необходимых для работы Системы;
- активацию необходимых лицензий.

В случае обнаружения сбоев в работе Системы по причине ошибок, не связанных с объектами ИТ инфраструктуры Заказчика, Исполнитель обязуется внести коррективы в функционал продукта до подписания акта о выполненных работах.

3.3 Порядок контроля и приемка Системы

Приемка Системы должна производится путем проведения приемочных испытаний. Приемочные испытания осуществляются представителями Заказчика и Исполнителя.

Цель приемочных испытаний состоит в подтверждении работоспособности компонентов Системы и соответствие их требованиям ТЗ.

Виды, состав, объем и методы испытаний должны определяться программой приемочных испытаний. Программа приемочных испытаний разрабатывается Исполнителем и согласовывается Заказчиком не позднее, чем за 1 день перед началом испытаний.

Результаты приемочных испытаний должны оформляться протоколом, который подписывается членами приемочной комиссии. По факту успешного проведения приемочных испытаний подписывается Акт завершения приемочных испытаний.

При обнаружении во время приемочных испытаний недостатков, дефектов или иных отклонений от требований ТЗ, соответствующие факты должны фиксироваться в протоколе, в котором в том числе указывается:

- перечень недостатков (дефектов);
- степень влияния отмеченных недостатков на работоспособность системы;
- требуемые сроки устранения недостатков (дефектов).

В течение пяти рабочих дней с момента устранения недостатков, дефектов или иных отклонений от требований к системе, приемочная комиссия должна провести повторные приёмочные испытания соответствующего компонента и принять Системы в постоянную эксплуатацию.

3.4 Обучение персонала.

Обучение согласно п.9 данного ТЗ.

4 Место выполнения работ и оказания услуг

Исполнитель должен обеспечить поставку, инсталляцию и настройку ПО, по следующему адресу: Республика Узбекистан, г. Ташкент, 100000, проспект Амира Темура, 24, Центральный офис ООО «UMS».

Сроки поставки Системы будут определены в Договоре между Заказчиком и Исполнителем, но не более 90 календарных дней, со дня подписания договорных отношений Заказчика с Исполнителем.

5 Технические требования к Системе

К Системе предъявляются следующие основные технические требования.

5.1 Общие требования

5.1.1 Предлагаемая система должна относиться к классу SIEM (Security Information and Event Management) и обеспечивать централизованный сбор, хранение, обработку, индексирование, поиск, корреляцию и анализ событий информационной безопасности и ИТ-инфраструктуры.

5.1.2 Система должна предоставлять единый интерфейс и единое хранилище данных для задач логгирования, мониторинга безопасности, расследования инцидентов, отчетности, визуализации и администрирования.

5.1.3 Система должна обеспечивать сохранение исходных данных с возможностью последующего поиска и анализа, при этом предварительная нормализация не должна быть обязательным условием приема данных.

5.1.4 Система должна обеспечивать работу с разнородными машинными данными без необходимости предварительного преобразования всех источников в единую реляционную модель.

5.1.5 Решение должно иметь подтвержденную практику промышленного применения у крупных корпоративных заказчиков и развитую экосистему документации, профессиональных сервисов, обучения, поддержки и партнеров.

5.1.6 Лицензирование решения должно быть прозрачным и позволять масштабирование по объему обрабатываемых/индексируемых данных и/или функциональным модулям без необходимости полной замены архитектуры.

5.2 Архитектура и масштабируемость

5.2.1 Решение должно быть программным и не должно требовать обязательного использования специализированных физических устройств производителя.

5.2.2 Система должна поддерживать развертывание в физической инфраструктуре, виртуальной среде, частном/публичном облаке либо в гибридной модели.

5.2.3 Система должна поддерживать распределенную архитектуру для центральной площадки и удаленных площадок, включая сбор, буферизацию, передачу и централизованную обработку данных.

5.2.4 Архитектура должна поддерживать горизонтальное масштабирование компонентов сбора, индексирования/хранения и поиска без полной переустановки системы.

5.2.5 Система должна обеспечивать распределенный поиск по нескольким узлам хранения/индексации и поддерживать параллельную обработку поисковых запросов.

5.2.6 Система должна поддерживать размещение разных типов данных в отдельных логических хранилищах для оптимизации производительности поиска, разграничения доступа и управления сроками хранения.

5.2.7 Система должна поддерживать обработку крупных объемов машинных данных и

иметь документально подтвержденную возможность масштабирования до десятков ТБ данных в сутки при соответствующем проектировании инфраструктуры.

5.3 Требования к сбору, приему и интеграции данных

5.3.1 Система должна обеспечивать сбор данных по протоколам Syslog, TCP/UDP, защищенным каналам TLS/SSL, через агентское ПО, API/REST, WMI, SNMP events, из файлов журналов, JSON, XML, CSV, баз данных, скриптовых и модульных источников.

5.3.2 Агентское ПО должно поддерживать шифрование передачи данных, кэширование при недоступности центральных компонентов, балансировку нагрузки между принимающими узлами и передачу данных по надежному транспортному протоколу.

5.3.3 Система должна поддерживать как агентские, так и безагентные методы сбора данных, включая прямой доступ к логам по сети, прием от существующих Syslog-серверов и интеграцию через API.

5.3.4 Система должна поддерживать индексирование многострочных и сложных событий без потери структуры события и исходной временной метки.

5.3.5 Система не должна требовать предварительного описания структуры каждого источника до начала приема данных.

5.3.6 Система должна обеспечивать прием, индексирование и хранение исходных, немодифицированных машинных данных из любых источников.

5.3.7 Система должна корректно обрабатывать временные метки из разных часовых поясов и сохранять оригинальное время события наряду со временем поступления в систему.

5.3.8 Система не должна зависеть исключительно от готовых коннекторов производителя: должна быть возможность подключать новые источники и адаптироваться к изменению форматов логов без изменения исходного кода продукта.

5.3.9 Должна поддерживаться автоматическая проверка доступности источников, контроль полноты поступающих событий и оповещение при прекращении поступления данных от критичных источников.

5.3.10 Система должна поддерживать интеграцию с Active Directory/LDAP, системами аутентификации, межсетевыми экранами, IDS/IPS, WAF, VPN, EDR/XDR/антивирусами, DLP, сканерами уязвимостей, почтовыми и веб-шлюзами, DNS/DHCP, сетевыми устройствами, NetFlow/IPFIX, операционными системами, базами данных, системами виртуализации, облачными сервисами, бизнес-приложениями, Service Desk/ITSM, CMDB и пользовательскими приложениями.

5.4 Требования к хранению, индексированию и жизненному циклу данных

5.4.1 Система должна индексировать исходные, немодифицированные машинные данные и обеспечивать последующий поиск, расследование и отчетность по этим данным.

5.4.2 Система должна поддерживать автоматическое сжатие индексированных данных для оптимизации использования дискового пространства.

5.4.3 Должна быть обеспечена возможность хранения оперативных, теплых и архивных данных с гибкой настройкой сроков хранения по типам источников, индексам, критичности и требованиям комплаенса.

5.4.4 Система должна поддерживать детализированное управление данными по мере их устаревания: перенос на более дешевое/внешнее хранилище, архивирование и/или удаление согласно политикам Заказчика.

5.4.5 Система должна поддерживать репликацию данных/индексов для обеспечения доступности, целостности, устойчивости к сбоям и повышения производительности поиска.

5.4.6 Должна быть обеспечена возможность масштабирования хранилища без остановки всей системы.

5.4.7 Должна быть обеспечена защита журналов и аудиторских данных от несанкционированного изменения и удаления, включая механизмы проверки целостности.

5.5 Требования к нормализации, обогащению и контексту

5.5.1 Система должна поддерживать нормализацию событий к унифицированной модели данных для типовых сценариев безопасности, при этом исходные сырые данные должны оставаться доступными для поиска и расследования.

5.5.2 Изменение логики извлечения полей, справочников, правил нормализации или обогащения не должно требовать обязательной повторной загрузки ранее сохраненных событий.

5.5.3 Система должна поддерживать категоризацию событий и обогащение событий дополнительными данными (контекст, справочники, списки активов, информация о пользователях, данные AD/IDM, внешние и внутренние виды угроз и иные справочные источники).

5.5.4 Должна поддерживаться интеграция с корпоративными директориями для получения атрибутов пользователей: логин, ФИО, подразделение, должность, руководитель, телефон, местоположение, признак привилегированности, даты начала/окончания работы и иные атрибуты.

5.5.5 Должна поддерживаться корреляция нескольких учетных записей/логинов с одним сотрудником или субъектом.

5.5.6 Должна поддерживаться интеграция с базами активов (CMDB) для получения информации об устройствах: hostname, IP, MAC, местоположение, владелец, критичность, наличие чувствительных данных, соответствие регуляторным требованиям.

5.5.7 Система должна позволять применять новые справочники и контекстные данные к ранее проиндексированным событиям для поиска и отчетности за прошлые периоды.

5.6 Требования к поиску, аналитике и корреляции

5.6.1 Система должна поддерживать интерактивный полнотекстовый поиск по любому полю индексированных данных с использованием ключевых слов, временных интервалов, логических операторов, регулярных выражений и подстановочных символов.

5.6.2 Система должна поддерживать как поиски в реальном времени, так и запланированные поиски, а также параллельное выполнение нескольких поисковых запросов.

5.6.3 В системе должно быть наличие возможности выполнять поиск, расследование, корреляцию и построение отчетности непосредственно по исходным индексированным событиям, без предварительной нормализации или загрузки данных в отдельную SQL-базу данных, рассматривается как дополнительное преимущество системы.

5.6.4 Система должна поддерживать подход, при котором исходные события сохраняются в полном виде, а извлечение полей, нормализация, обогащение и интерпретация данных могут выполняться как на этапе приема, так и на этапе поиска и анализа ранее сохраненных данных.

5.6.5 Система должна позволять сохранять, редактировать, повторно использовать и передавать поисковые запросы другим пользователям с учетом ролевой модели доступа.

5.6.6 Система должна поддерживать статистический анализ: подсчет, уникальные значения, сумма, минимум, максимум, среднее, медиана, мода, стандартное отклонение, дисперсия, перцентили, первое/последнее появление значения.

5.6.7 Система должна поддерживать выявление редких и аномальных значений, построение базовых профилей поведения и выявление отклонений, включая сценарии неизвестных угроз и APT без жесткой зависимости от сигнатур.

5.6.8 Система должна поддерживать корреляцию событий по временным, логическим, поведенческим и статистическим правилам, включая многошаговые сценарии атак.

5.6.9 Система должна поддерживать использование моделей kill chain, MITRE ATT&CK или аналогичных фреймворков для классификации и описания сценариев выявления.

5.6.10 Система должна позволять создавать собственные правила корреляции, изменять существующие правила и тестировать их до ввода в промышленную эксплуатацию.

5.6.11 Система должна предоставлять преднастроенный SIEM-контент: корреляционные правила, дашборды, отчеты, модели данных, сценарии расследования и шаблоны мониторинга безопасности с возможностью адаптации под инфраструктуру Заказчика.

5.7 Требования к мониторингу, оповещениям и расследованию инцидентов

5.7.1 Система должна поддерживать мониторинг в режиме, близком к реальному времени, и формирование оповещений по результатам поисков, корреляционных правил и аналитических сценариев.

5.7.2 Оповещения должны поддерживать настройку приоритетов, подавление повторных срабатываний, ограничение частоты срабатывания и маршрутизацию ответственным группам.

5.7.3 Система должна поддерживать отправку уведомлений по электронной почте, через интеграции с внешними системами, Webhook/API, запуск пользовательских скриптов либо иные механизмы автоматизации.

5.7.4 Система должна предоставлять рабочие процессы расследования инцидентов: карточка/объект инцидента, привязка исходных событий и контекста, история

расследования, статусы, комментарии, назначение ответственных и возможность документирования результатов.

5.7.5 Система должна обеспечивать переход от сводного события/дашборда/корреляционного срабатывания к исходным событиям для детального расследования.

5.8 Требования к визуализации и отчетности

5.8.1 Система должна поддерживать построение интерактивных дашбордов и отчетов, включая таблицы, временные диаграммы, линейные, столбчатые, площадные, круговые и точечные графики, индикаторы состояния и географические визуализации по IP/Geo-IP.

5.8.2 Визуализации должны поддерживать обновление в реальном времени, drill-down от агрегированных показателей к исходным событиям и выделение аномалий/выбросов.

5.8.3 Система должна позволять создавать отчеты и дашборды как техническим, так и нетехническим пользователям, включая визуальное редактирование панелей и настройку заголовков, легенд, осей и фильтров.

5.8.4 Система должна поддерживать формирование отчетов по расписанию и экспорт/рассылку отчетов в распространенные форматы, включая PDF, CSV, XLS/XLSX и иные форматы, доступные в продукте.

5.8.5 Система должна поддерживать отчеты и панели мониторинга для задач соответствия требованиям ИБ и регуляторики, включая ISO 27002, NIST, PCI DSS и аналогичные стандарты.

5.9 Требования к безопасности, доступу и аудиту

5.9.1 Система должна поддерживать гибкую ролевую модель доступа (RBAC) для пользователей и API с возможностью ограничения доступа к источникам данных, типам данных, временным диапазонам, отчетам, дашбордам, поискам и административным функциям.

5.9.2 Система должна поддерживать интеграцию с Active Directory/LDAP и корпоративными системами единого входа (SSO).

5.9.3 Передача данных между компонентами должна осуществляться по защищенным каналам с использованием современных криптографических протоколов.

5.9.4 Система должна вести полный аудит действий пользователей и администраторов: входы, поисковые запросы, просмотр отчетов, изменения конфигурации, управление пользователями, создание/изменение правил и иные значимые действия.

5.9.5 Аудиторские события должны содержать дату и время, пользователя/субъект, источник, выполненное действие и результат выполнения.

5.9.6 Система должна поддерживать механизмы подтверждения целостности индексированных событий, включая хеширование и/или цифровую подпись событий либо функционально эквивалентный механизм контроля подлинности.

5.9.7 Система должна обеспечивать мониторинг собственной конфигурации, доступности компонентов и состояния системных сервисов с возможностью оповещения о сбоях.

5.10 Открытость архитектуры и интеграция со сторонними системами

5.10.1 Система должна предоставлять открытые интерфейсы API для доступа к индексированным данным, выполнения поисковых запросов, управления объектами конфигурации и интеграции с внешними системами.

5.10.2 Система должна поддерживать SDK или иметь библиотеки для распространенных языков программирования, включая Python, Java, JavaScript, C# или аналогичные

5.10.3 Все конфигурации системы должны быть доступны для управления через веб-интерфейс, CLI и/или конфигурационные файлы.

5.10.4 Система должна поддерживать интеграцию с внешними системами визуализации, BI, ITSM/SOAR, CMDB, threat intelligence, системами мониторинга и иными корпоративными платформами Заказчика.

5.10.5 Система должна иметь возможность пересылать сырые, преобразованные или обогащенные события во внешние системы по Syslog TCP/UDP, raw TCP, через файл, API или аналогичный механизм.

5.10.6 Система должна поддерживать использование публичных и/или предоставляемых производителем приложений/пакетов интеграции для популярных продуктов и сценариев безопасности.

5.10.7 Система должна иметь официально поддерживаемый производителем механизм непосредственной интеграции с Palo Alto Networks Cortex XDR, реализованный в виде штатного приложения, Add-on, модуля или иного специализированного компонента SIEM.

5.10.8 Штатная интеграция должна обеспечивать автоматизированное получение из Cortex XDR взаимосвязанных данных, включающих как минимум: инциденты, alerts, детализированные события, сведения о конечных устройствах, пользователях, процессах, сетевых соединениях, объектах угроз, артефактах и статусах обработки инцидентов.

5.10.9 Интеграция должна обеспечивать получение как агрегированных данных об инцидентах, так и связанных с ними детализированных событий и телеметрии, с сохранением взаимосвязи между исходным событием, alert и соответствующим инцидентом Cortex XDR.

5.10.10 Полученные данные Cortex XDR должны автоматически преобразовываться средствами штатной интеграции в единую нормализованную модель данных SIEM с сохранением исходных значений и взаимосвязей между объектами.

5.10.11 Нормализованные данные Cortex XDR должны непосредственно использоваться основными механизмами SIEM, включая поиск, корреляцию, аналитические правила, визуализацию, расследование инцидентов, риск-ориентированный анализ и security content, без необходимости дополнительного преобразования данных.

5.10.12 SIEM должен обеспечивать автоматическое сопоставление данных Cortex XDR с объектами Asset и Identity, включая endpoint, IP-адрес, DNS-имя, учетную запись пользователя и иные идентификаторы, с возможностью использования данного контекста при последующем анализе.

5.10.13 Данные Cortex XDR должны непосредственно участвовать в штатном механизме риск-ориентированного анализа SIEM с возможностью формирования,

накопления и агрегирования риск-событий для пользователей, конечных устройств и иных объектов.

5.10.14 SIEM должен обеспечивать автоматическое объединение событий Cortex XDR с событиями иных источников в едином аналитическом контексте на основании временных, идентификационных, сетевых и иных взаимосвязей.

5.10.15 SIEM должен обеспечивать формирование единого инцидента или аналитического объекта на основании совокупности событий Cortex XDR и событий иных подключенных источников без необходимости создания отдельного аналитического контура для данных Cortex XDR.

5.10.16 Данные Cortex XDR должны использоваться в преднастроенном security content, поставляемом производителем SIEM, включая корреляционные правила, аналитические сценарии, правила обнаружения угроз и иные механизмы анализа, без необходимости разработки Заказчиком специализированных механизмов преобразования данных Cortex XDR.

5.10.17 SIEM должен обеспечивать сквозную связь:

- Cortex XDR event → нормализованное событие SIEM → Asset/Identity → Risk → Correlation → Incident
- с возможностью перехода между указанными объектами в рамках единого интерфейса расследования.

5.10.18 При расследовании инцидента SIEM должен обеспечивать drill-down от агрегированного инцидента, корреляционного события или объекта риска до исходных данных Cortex XDR с отображением связанных endpoint, пользователя, процесса, файла, IP-адреса, домена, сетевого соединения и иных доступных атрибутов.

5.10.19 SIEM должен обеспечивать возможность выполнения исторического поиска и ретроспективного анализа данных Cortex XDR совместно с данными иных источников без повторного получения исходных данных из Cortex XDR.

5.10.20 SIEM должен обеспечивать применение изменённых или вновь созданных правил нормализации, классификации, обогащения и корреляции к ранее полученным данным Cortex XDR без необходимости повторной загрузки исторического массива данных.

5.10.21 Данные Cortex XDR должны быть доступны для построения оперативных и исторических dashboards и аналитических представлений совместно с данными других источников с возможностью drill-down до исходного события.

5.10.22 Система должна обеспечивать использование данных Cortex XDR в аналитике угроз и MITRE ATT&CK с возможностью отображения соответствующих тактик, техник и связанных событий в рамках единого расследования.

5.10.23 Система должна обеспечивать контроль работоспособности штатного компонента интеграции Cortex XDR, включая контроль состояния подключения, получения данных, ошибок обработки, задержек поступления данных и признаков прекращения поступления данных.

5.10.24 Для реализации требований 5.10.7–5.10.25 не допускается обязательное использование самостоятельно разработанных Заказчиком скриптов, парсеров, ETL-процедур, промежуточных баз данных либо иных программных компонентов, не входящих в штатную поддерживаемую производителем

интеграцию SIEM с Cortex XDR.

5.10.25 Все указанные механизмы должны функционировать в рамках единого технологического контура SIEM и не должны требовать передачи данных Cortex XDR в отдельную аналитическую платформу для реализации нормализации, корреляции, риск-анализа, визуализации или расследования.

5.11 Требования к отказоустойчивости и режимам функционирования

5.11.1 Система должна поддерживать резервирование ключевых компонентов, кластеризацию, репликацию критичных данных и отсутствие единой точки отказа при целевой архитектуре N+1.

5.11.2 Система должна обеспечивать автоматическое восстановление либо документированную процедуру восстановления при сбоях компонентов.

5.11.3 Основной режим функционирования Системы – непрерывная круглосуточная работа в автоматизированном режиме под управлением администратора.

5.11.4 Система должна поддерживать штатный, сервисный и автономный режимы, включая возможность локальной буферизации данных при временной недоступности центральных компонентов.

5.12 Требования к производительности и пропускной способности

Поставляемое решение должно отвечать следующим требованиям:

№	Показатель	Требуемое значение
1	Средняя производительность по приему событий (EPS)	не менее 80 000 EPS либо эквивалентный объем данных, рассчитанный по среднему размеру события
2	Пиковая производительность по приему событий	не менее 150 000 EPS
3	Возможность кратковременного burst-нагрузки	до 250 000 EPS без потери событий при корректно рассчитанной архитектуре и буферизации
4	Суточный объем индексируемых данных	не менее 100 ГБ/сутки с возможностью дальнейшего увеличения без смены платформы
5	Объем хранения «горячих» данных (оперативный доступ)	не менее 180 суток
6	Объем хранения «тёплых» данных	не менее 12 месяцев
7	Общий срок хранения архивных данных	не менее 3 лет
8	Максимальная задержка обработки события до оповещения	не более 3 секунд для критичных корреляционных сценариев при штатной нагрузке
9	Потери событий при штатной нагрузке	0% при корректной настройке источников и каналов передачи
10	Количество одновременно подключенных источников	не менее 2 000

№	Показатель	Требуемое значение
11	Поддержка распределённых коллекторов/агентов	не менее 10 удалённых площадок
12	Количество одновременно работающих пользователей SOC	не менее 20
13	Время выполнения поискового запроса по данным за 90 суток	не более 120 секунд для согласованных типовых поисковых запросов
14	Время выполнения агрегационного отчета за 6 месяцев	не более 10 минут
15	Масштабирование производительности	горизонтальное, без полной остановки системы
16	Возможность увеличения EPS	минимум в 3 раза без смены архитектурного подхода
17	Поддержка раздельного хранения (hot/warm/archive tiers)	обязательна
18	Отказоустойчивость	отсутствие единой точки отказа (N+1)

5.13 Требования к дополнительным сценариям использования

5.13.1 Система должна позволять использовать один раз собранные и индексированные данные в различных сценариях: мониторинг ИБ, комплаенс, расследование инцидентов, выявление мошенничества, IT-операции, мониторинг приложений, цифровая аналитика и бизнес-аналитика.

5.13.2 Система должна поддерживать расширение функциональности за счет дополнительных модулей, приложений или интеграций без необходимости миграции данных на отдельную платформу.

5.13.3 Система должна обеспечивать возможность последующего развития в сторону автоматизации реагирования, интеграции с SOAR/ITSM и расширенной аналитики поведения пользователей и сущностей.

6 Требования к Исполнителю

К Исполнителю предъявляются следующие требования:

6.1 В рамках закупочной процедуры Исполнитель должен предоставить детальную спецификацию поставляемого ПО;

6.2 Общие требования к Исполнителю

Исполнитель должен удовлетворять следующим требованиям:

- подтвержденный опыт работы по предоставлению обозначенных услуг (поставка ПО);
- являться авторизованным партнёром, а также иметь документальное подтверждение на распространение конечным пользователям прав на использование и внедрение реализуемого/внедряемого программного обеспечения;
- Исполнитель обязуется предоставить сертификат ГУП «Центр кибербезопасности» на предлагаемое ПО (на соответствие требованиям обеспечения информационной и кибербезопасности), либо, в случае его отсутствия, пройти процедуру сертификации ПО, на стадии внедрения проекта.

Исполнитель обязан соблюдать требования, предъявляемые действующим

законодательством Республики Узбекистан к работе с документами и сведениями, содержащими конфиденциальную информацию и не разглашать конфиденциальную информацию, ставшую ему известной в процессе оказания услуг.

6.3 Исполнитель должен включить в состав предложения следующие документы, подтверждающие его соответствие вышеуказанным требованиям:

- копию авторизированного письма о наличии партнерского статуса с компанией производителем;
- копии минимум 2-х сертификатов инженеров от компании производителя
- перечень реализованных ИТ-проектов.

7 Требования к безопасности выполнения работ и оказания услуг

Так как при реализации проекта будут использоваться только программные решения, то специальных требований по безопасности не предъявляется.

8 Требования по передаче технических и иных документов по результатам выполненных работ и оказанных услуг

После завершения внедрения и ввода Системы в промышленную эксплуатацию Исполнитель обязан подготовить рабочую (исполнительную) документацию**, отражающую** фактически реализованное состояние Системы**.**

Документация предоставляется:

- в 2 (двух) экземплярах на бумажном носителе;
- в электронном виде (форматы: DOCX и PDF).

Обязательный состав документации:

- общее описание Системы;
- архитектурные и сетевые схемы;
- перечень и конфигурация аппаратных и программных компонентов;
- описание интеграций с инфраструктурой Заказчика;
- сетевая адресация (IP, порты, протоколы);
- краткая эксплуатационная документация;
- описание реализованных мер информационной безопасности.

Документация должна быть актуальной, полной и соответствовать фактической реализации Системы, а также достаточной для её эксплуатации без привлечения Исполнителя.

9 Требования к обучению персонала Заказчика

В рамках данного ТЗ, Исполнитель обеспечивает следующие программы обучения;

a) сертифицированное обучение двух специалистов ИБ Заказчика по администрированию данного комплекса.

Количество слушателей: 2 человека.

Формат: очное / онлайн, с практическими занятиями.

Язык обучения: русский / английский.

Материалы: презентации, инструкции, лабораторные работы.

По итогам обучения Исполнитель предоставляет:

- учебные материалы;
- записи занятий;
- подтверждение прохождения обучения (сертификаты).

b) обучение пользователей системы.

Количество слушателей: до 10 человек.

Формат: демонстрационный + практический.

Цель обучения: освоение функциональных возможностей системы.

Факт прохождения обучения должен быть подтвержден соответствующим сертификатом.

Программу и время обучения предварительно согласовать с Заказчиком.

10 Гарантийные обязательства

Исполнитель должен гарантировать, что качество выполненной работы будет соответствовать техническому заданию и требованиям указанными Заказчиком, при условии соблюдения правил эксплуатации программного (программно-аппаратного) обеспечения, установленных производителем в документации и отсутствия несанкционированного вмешательства в работу инсталлированного программного обеспечения.

Срок гарантии на выполненные работы по внедрению Системы, должен составлять **12 (двенадцать) месяцев** и исчисляется со дня подписания Сторонами акта сдачи – приемки работ.

Срок подписки (Subscription) на лицензии должен составлять **12 (двенадцать) месяцев.**

Период опытной эксплуатации должен составлять 1 (один) месяц и исчисляться со дня подписания Сторонами акта сдачи – приемки работ.

11 Условия сервисной поддержки и техническое сопровождение

Срок сервисной поддержки производителя – **12 (двенадцать) месяцев**, с момента внедрения ПО. Сервисная поддержка на программные компоненты должна оказываться как производителем, так и Исполнителем.

Исполнитель обязан предоставить информацию об информационных ресурсах компании производителя ПО, для самостоятельного скачивания документации, обновлений, релизов.

Исполнитель осуществляет привязку идентификационных данных ПО в кабинете Заказчика, на сайте Производителя.

Работы по техническому сопровождению ПО должны включать в себя:

a) Обеспечение непрерывного функционирования серверной части Системы SIEM:

- настройка параметров Системы для оптимизации использования аппаратных и программных ресурсов;
- настройка параметров Системы для управления политикой безопасности;
- тестирование работы Системы в штатном режиме после проведения обновлений.

b) Интеграция с существующими системами управления и мониторинга.

c) Консультации по масштабированию Системы.

d) Доступ к порталу производителя ПО (возможность скачивать обновления, доступ к техническому форуму, доступ к документации).

e) Проведение инструктажа 2-х администраторов Системы в случае обновления Системы.

f) Подключение специалиста посредством VPN по требованию ООО «UMS» для решения возникших проблем, консультаций, связанных с функционированием Системы.

g) Восстановление работоспособности программного комплекса:

- восстановление работоспособности Системы в штатном режиме не позднее, чем через 2 рабочих дня после сбоя программных средств;
- перенастройка, реконфигурирование, обновление и/или полная переустановка программного комплекса, а также устранение причин, приведших к сбою (при условии сбоя, вызванного продуктами компании);
- возможность отключения Системы на время сбоя для проведения восстановительных работ (режим байпас);
- восстановление активности Системы, после аппаратных сбоев, потеря питания, и т.д.;

- операции восстановления данных из резервных копий.
- предоставление отчетов о проделанной работе.

12 Требования к технической поддержке

12.1 Исполнитель обязан обеспечить техническую поддержку поставляемого программного комплекса в течение 12 месяцев.

12.2 Поддержка должна оказываться производителем ПО либо авторизованным сервисным партнёром производителя.

12.3 Уровень поддержки должен предусматривать возможностью эскалации на уровень производителя (L3).

12.4 Поддержка должна распространяться на:

- программную часть (software).

12.5 Поддержка должна предоставляться в режиме:

- 24×7×365 – для критичных инцидентов;
- не ниже 8×5 – для некритичных (по согласованию с Заказчиком).

12.6 Время реакции на инциденты:

- Критический (P1): не более 60 минут;
- Высокий (P2): не более 2 часов;
- Средний (P3): не более 4 часов;
- Низкий (P4): не более 1 рабочего дня.

12.7 Время восстановления (или обходного решения):

- P1: не более 4 часов;
- P2: не более 8 часов;
- P3: до 2 рабочих дней;
- P4: по согласованию с Заказчиком.

12.8 Исполнитель должен предоставлен единый канал регистрации заявок на ТП:

- Service Desk (портал);
- телефон горячей линии;
- e-mail.

13 Иные требования к работам, услугам и условиям их оказания

13.1 Лицензии/ПО считаются принятым после проведения физической инвентаризации и работоспособности программного обеспечения в присутствии представителей сторон и соответствующего подписания Акта приема-передачи согласно заключенного договора. Другие условия, не указанные в данном ТЗ и его приложениях, будут указаны в контракте.

13.2 Обязательным условием оказания услуг является соблюдение правил действующего внутреннего распорядка Заказчика, контрольно-пропускного режима, внутренних положений, инструкций и требований, о которых Заказчик уведомит Исполнителя. Заказчик предоставляет Исполнителю список и контактные данные персонала, уполномоченного им на контакты с Исполнителем по решению заявленных проблем, связанных с активацией подписки на ПО.

13.3 Детальная форма подачи предложения представлена в Приложении №2 к данному ТЗ.

13.4 Требование к комплектации

Система должна иметь полную комплектацию, для полноценного функционирования предлагаемого решения в рамках текущего ТЗ. Стоимость ПО должна формироваться исходя из полной комплектации.

13.5 Требование к интеграции

Интеграция должна учитывать особенности работы инфраструктуры Заказчика.

13.6 Сведения о новизне

Поставляемое ПО должна быть актуальной последней версии, со всеми необходимыми лицензиями на продукт и его составляющими.

13.7 Страхование

Требования не предъявляются, однако Исполнитель несет ответственность сохранности программного (аппаратно-программного) комплекса до момента его официальной передачи Заказчику.

13.8 Матрица распределения ответственности при оказании

Техническое обслуживание	**Исполнитель**	**Заказчик**
Доступность системы		
Обнаружение и классификация приоритетности проблемы, открытие запроса для решения у Правообладателя	A	R
Производить настройку ПО Заказчика по запросу	A	R
Предоставлять статистику решения проблем за отчетный период	R	A
Регистрировать все запросы на портале Правообладателя	R	A
Обновления, исправления, корректировки программного обеспечения		
Предоставить метод процедуры	R	A
Определить время установки	A	R
Установить Программное обеспечения	R	A
Проверить работу установленного программного обеспечения	A	R
Сервисы и рекомендации		
Предоставить технические требования	R	R
Внедрение технических требований	R	A
Предоставить технические рекомендации	R	I

R (от англ. Responsible) – непосредственный исполнитель;
A (от англ. Accountable) – ответственное лицо, которое руководит работой исполнителя;
C (от англ. Consulted) – консультант (специалист либо эксперт в предметной области, к чьей помощи прибегает ответственное лицо до принятия конкретных решений);
I (от англ. Informed) – наблюдатель, информируемое лицо (лицо, которое надлежит уведомлять о ходе (либо результатах) выполнения задачи)

14 Используемые термины и сокращения

№	Термин / Сокращение	Расшифровка	Определение
1	SIEM	Security Information and Event Management	Система централизованного сбора, хранения, корреляции и анализа событий ИБ
2	SOC	Security Operations Center	Центр мониторинга и реагирования на инциденты ИБ
3	EPS	Events Per Second	Количество обрабатываемых событий в секунду
4	LPS	Logs Per Second	Количество логов, поступающих в систему в секунду
5	GB/day	Gigabytes per day	Суточный объём поступающих данных
6	Correlation	Корреляция событий	Связывание нескольких событий в единый

№	Термин / Сокращение	Расшифровка	Определение
			инцидент
7	Use Case	Сценарий выявления	Набор правил выявления определённого типа угрозы
8	Rule	Правило корреляции	Логическое условие выявления подозрительной активности
9	Incident	Инцидент ИБ	Подтверждённое событие нарушения ИБ
10	Event	Событие	Зафиксированное действие или состояние системы
11	Log	Журнал событий	Запись о событии в информационной системе
12	Parsing	Парсинг	Преобразование логов в структурированный формат
13	Normalization	Нормализация	Приведение событий к единой структуре
14	Enrichment	Обогащение данных	Добавление контекстной информации к событию
15	IOC	Indicator of Compromise	Индикатор компрометации (IP, hash, домен и др.)
16	MITRE ATT&CK	-	База знаний тактик и техник кибератак
17	UEBA	User and Entity Behavior Analytics	Анализ поведенческих аномалий пользователей и объектов
18	SOAR	Security Orchestration, Automation and Response	Оркестрация и автоматизация реагирования
19	XDR	Extended Detection and Response	Расширенная система выявления и реагирования
20	EDR	Endpoint Detection and Response	Система выявления угроз на рабочих станциях
21	NTA	Network Traffic Analysis	Анализ сетевого трафика
22	NetFlow	—	Протокол сбора статистики сетевого трафика
23	Syslog	—	Протокол передачи логов
24	API	Application Programming Interface	Интерфейс программного взаимодействия систем
25	AD	Active Directory	Служба каталогов Microsoft
26	LDAP	Lightweight Directory Access Protocol	Протокол доступа к службе каталогов
27	RBAC	Role-Based Access Control	Разграничение доступа на основе ролей
28	MFA	Multi-Factor Authentication	Многофакторная аутентификация
29	SLA	Service Level Agreement	Соглашение об уровне обслуживания
30	MTTR	Mean Time To Respond/Recover	Среднее время реагирования/восстановления
31	MTTD	Mean Time To Detect	Среднее время обнаружения угрозы
32	HA	High Availability	Отказоустойчивость
33	DR	Disaster Recovery	План восстановления после сбоя
34	Hot Storage	-	Быстрое (оперативное) хранение данных
35	Warm Storage	-	Промежуточное хранилище
36	Cold Storage	-	Архивное хранилище
38	Cluster	Кластер	Группа серверов, работающих как единая система

№	Термин / Сокращение	Расшифровка	Определение
39	Node	Узел	Отдельный сервер в кластере
40	Dashboard	Дашборд	Панель визуализации событий и показателей

15 Перечень приложений

Приложение №1 – Характеристика объекта информатизации.
Приложение №2 – Таблица соответствия техническим требованиям.

ТЗ разработал:

Начальник отдела информационной безопасности ДИБиР _____ (подпись) Абдульваат Р.А.

Директор ДИБиР _____ (подпись) Олматов Б.А.

Приложение 1

Характеристики объекта информатизации

ООО «UMS» - телекоммуникационная компания, оказывающая услуги мобильной связи на всей территории Республики Узбекистан с 1 декабря 2014 года.

ООО «UMS» образован на основании постановления Кабинета Министров Республики Узбекистан №208 «О создании совместного предприятия «Universal Mobile Systems» по оказанию услуг мобильной связи» от 31 июля 2014 года, является одним из ведущих мобильных операторов Республики Узбекистан.

В соответствии с Постановлением Президента Республики Узбекистан №ПП-5187 от 19 июля 2021г. учредителем ООО «UMS» является Министерство по развитию информационных технологий и коммуникаций Республики Узбекистан.

Штатная численность Компании, 1800 человек.

Общее количество серверов (в т.ч. виртуальны) – не более 1000 шт.

Общее количество сетевых устройств – не более 150 шт.

Общее количество приложений – 10

Общее количество информационных программных средств ИБ – не менее 10

Общая пропускная способность – не более 1000 Мбит/с.

Суммарный объем генерируемых логов – не более 100 Гб/сутки.

Приложение 2

Таблица соответствия техническим требованиям

№ требования	Наименование требования/ технические характеристики
1	ПО поставляется с лицензиями по подписке сроком на 12 месяцев (Лицензирование решения - прозрачное и позволять масштабирование по объему обрабатываемых/индексируемых данных и/или функциональным модулям без необходимости полной замены архитектуры)
2	ПО (решение) должно относится к классу SIEM (Security Information and Event Management)
3	Система должна предоставлять единый интерфейс и единое хранилище данных для задач логгирования, мониторинга безопасности, расследования инцидентов, отчетности, визуализации и администрирования.
4	Система должна обеспечивать сохранение исходных данных с возможностью последующего поиска и анализа, при этом предварительная нормализация не должна быть обязательным условием приема данных
5	Система должна обеспечивать работу с разнородными машинными данными без необходимости предварительного преобразования всех источников в единую реляционную модель
6	Решение должно иметь подтвержденную практику промышленного применения у крупных корпоративных заказчиков и развитую экосистему документации, профессиональных сервисов, обучения, поддержки и партнеров
7	Система поддерживает развертывание в физической инфраструктуре, виртуальной среде, частном/публичном облаке либо в гибридной модели и не требует обязательного использования специализированных физических устройств производителя
8	Архитектура решения поддерживает горизонтальное масштабирование компонентов сбора, индексирования/хранения и поиска без полной переустановки системы
9	Система обеспечивает распределенный поиск по нескольким узлам хранения/индексации и поддерживать параллельную обработку поисковых запросов
10	Система поддерживает размещение разных типов данных в отдельных логических хранилищах для оптимизации производительности поиска, разграничения доступа и управления сроками хранения
11	Система поддерживает обработку крупных объемов машинных данных и иметь документально подтвержденную возможность масштабирования до десятков ТБ данных в сутки при соответствующем проектировании инфраструктуры
12	Система обеспечивает сбор данных по протоколам Syslog, TCP/UDP, защищенным каналам TLS/SSL, через агентское ПО, API/REST, WMI, SNMP events, из файлов журналов, JSON, XML, CSV, баз данных, скриптовых и модульных источников.
13	Агентское ПО поддерживает шифрование передачи данных, кэширование при недоступности центральных компонентов, балансировку нагрузки между принимающими узлами и передачу данных по надежному транспортному протоколу
14	Система поддерживает как агентские, так и безагентные методы сбора данных, включая прямой доступ к логам по сети, прием от существующих Syslog-серверов и интеграцию через API

15	Система поддерживает индексирование многострочных и сложных событий без потери структуры события и исходной временной метки
16	Система не должна требовать предварительного описания структуры каждого источника до начала приема данных
17	Система должна обеспечивать прием, индексирование и хранение исходных, немодифицированных машинных данных из любых источников
18	Система корректно обрабатывает временные метки из разных часовых поясов и сохранять оригинальное время события наряду со временем поступления в Систему
19	Система не зависит исключительно от готовых коннекторов производителя: должна быть возможность подключать новые источники и адаптироваться к изменению форматов логов без изменения исходного кода продукта
20	Поддерживаться автоматическая проверка доступности источников, контроль полноты поступающих событий и оповещение при прекращении поступления данных от критичных источников.
21	Система поддерживает интеграцию с Active Directory/LDAP, системами аутентификации, межсетевыми экранами, IDS/IPS, WAF, VPN, EDR/XDR/антивирусами, DLP, сканерами уязвимостей, почтовыми и веб-шлюзами, DNS/DHCP, сетевыми устройствами, NetFlow/IPFIX, операционными системами, базами данных, системами виртуализации, облачными сервисами, бизнес-приложениями, Service Desk/ITSM, CMDB и пользовательскими приложениями
22	Система индексирует исходные, немодифицированные машинные данные и обеспечивает последующий поиск, расследование и отчетность по этим данным, а также поддерживает автоматическое сжатие индексированных данных для оптимизации использования дискового пространства
23	В Системе присутствует возможность хранения оперативных, теплых и архивных данных с гибкой настройкой сроков хранения по типам источников, индексам, критичности и требованиям комплаенса
24	Система поддерживает детализированное управление данными по мере их устаревания: перенос на более дешевое/внешнее хранилище, архивирование и/или удаление согласно политикам Заказчика
25	Система поддерживает репликацию данных/индексов для обеспечения доступности, целостности, устойчивости к сбоям и повышения производительности поиска
26	Существует возможность масштабирования хранилища без остановки всей Системы
27	Существует защита журналов и аудиторских данных от несанкционированного изменения и удаления, включая механизмы проверки целостности
28	Система поддерживает нормализацию событий к унифицированной модели данных для типовых сценариев безопасности, при этом исходные сырые данные должны оставаться доступными для поиска и расследования
29	Изменение логики извлечения полей, справочников, правил нормализации или обогащения не требует обязательной повторной загрузки ранее сохраненных событий
30	Система поддерживает категоризацию событий и обогащение событий дополнительными данными (контекст, справочники, списки активов, информация о пользователях, данные AD/IDM, внешние и внутренние виды угроз и иные справочные источники)
31	Поддерживается интеграция с корпоративными директориями для получения атрибутов пользователей: логин, ФИО, подразделение, должность,

	руководитель, телефон, местоположение, признак привилегированности, даты начала/окончания работы и иные атрибуты
32	Поддерживаются корреляция нескольких учетных записей/логинов с одним сотрудником или субъектом
33	Поддерживается интеграция с базами активов (CMDB) для получения информации об устройствах: hostname, IP, MAC, местоположение, владелец, критичность, наличие чувствительных данных, соответствие регуляторным требованиям
34	Система позволяет применять новые справочники и контекстные данные к ранее проиндексированным событиям для поиска и отчетности за прошлые периоды
35	Система поддерживает интерактивный полнотекстовый поиск по любому полю индексированных данных с использованием ключевых слов, временных интервалов, логических операторов, регулярных выражений и подстановочных символов
36	Система поддерживает как поиски в реальном времени, так и запланированные поиски, а также параллельное выполнение нескольких поисковых запросов
37	Система поддерживает подход, при котором исходные события сохраняются в полном виде, а извлечение полей, нормализация, обогащение и интерпретация данных могут выполняться как на этапе приема, так и на этапе поиска и анализа ранее сохраненных данных
38	Система позволяет сохранять, редактировать, повторно использовать и передавать поисковые запросы другим пользователям с учетом ролевой модели доступа
39	Система поддерживает статистический анализ: подсчет, уникальные значения, сумма, минимум, максимум, среднее, медиана, мода, стандартное отклонение, дисперсия, перцентили, первое/последнее появление значения
40	Система поддерживает выявление редких и аномальных значений, построение базовых профилей поведения и выявление отклонений, включая сценарии неизвестных угроз и APT без жесткой зависимости от сигнатур
41	Система поддерживает корреляцию событий по временным, логическим, поведенческим и статистическим правилам, включая многошаговые сценарии атак
42	Система поддерживает использование моделей kill chain, MITRE ATT&CK или аналогичных фреймворков для классификации и описания сценариев выявления
43	Система позволяет создавать собственные правила корреляции, изменять существующие правила и тестировать их до ввода в промышленную эксплуатацию
44	Система предоставляет преднастроенный SIEM-контент: корреляционные правила, дашборды, отчеты, модели данных, сценарии расследования и шаблоны мониторинга безопасности с возможностью адаптации под инфраструктуру Заказчика
45	Система поддерживает мониторинг в режиме, близком к реальному времени, и формирование оповещений по результатам поисков, корреляционных правил и аналитических сценариев
46	Оповещения поддерживают настройку приоритетов, подавление повторных срабатываний, ограничение частоты срабатывания и маршрутизацию ответственным группам
47	Система поддерживает отправку уведомлений по электронной почте, через интеграции с внешними системами, Webhook/API, запуск пользовательских скриптов либо иные механизмы автоматизации

48	Система предоставляет рабочие процессы расследования инцидентов: карточка/объект инцидента, привязка исходных событий и контекста, история расследования, статусы, комментарии, назначение ответственных и возможность документирования результатов
49	Система обеспечивает переход от сводного события/дашборда/корреляционного срабатывания к исходным событиям для детального расследования
50	Система поддерживает построение интерактивных дашбордов и отчетов, включая таблицы, временные диаграммы, линейные, столбчатые, площадные, круговые и точечные графики, индикаторы состояния и географические визуализации по IP/Geo-IP
51	Визуализации поддерживают обновление в реальном времени, drill-down от агрегированных показателей к исходным событиям и выделение аномалий/выбросов
52	Система позволяет создавать отчеты и дашборды как техническим, так и нетехническим пользователям, включая визуальное редактирование панелей и настройку заголовков, легенд, осей и фильтров
53	Система поддерживает формирование отчетов по расписанию и экспорт/рассылку отчетов в распространенные форматы, включая PDF, CSV, XLS/XLSX и иные форматы, доступные в продукте
54	Система поддерживает отчеты и панели мониторинга для задач соответствия требованиям ИБ и регуляторики, включая ISO 27002, NIST, PCI DSS и аналогичные стандарты
55	Система поддерживает гибкую ролевую модель доступа (RBAC) для пользователей и API с возможностью ограничения доступа к источникам данных, типам данных, временным диапазонам, отчетам, дашбордам, поискам и административным функциям
56	Система поддерживает интеграцию с Active Directory/LDAP и корпоративными системами единого входа (SSO)
57	Передача данных между компонентами осуществляется по защищенным каналам с использованием современных криптографических протоколов
58	Система ведет полный аудит действий пользователей и администраторов: входы, поисковые запросы, просмотр отчетов, изменения конфигурации, управление пользователями, создание/изменение правил и иные значимые действия
59	Аудиторские события Системы содержат дату и время, пользователя/субъект, источник, выполненное действие и результат выполнения
60	Система поддерживает механизмы подтверждения целостности индексированных событий, включая хеширование и/или цифровую подпись событий либо функционально эквивалентный механизм контроля подлинности
61	Система обеспечивает мониторинг собственной конфигурации, доступности компонентов и состояния системных сервисов с возможностью оповещения
62	Система предоставляет открытые интерфейсы API для доступа к индексированным данным, выполнения поисковых запросов, управления объектами конфигурации и интеграции с внешними системами
63	Система должна поддерживать SDK или иметь библиотеки для распространенных языков программирования, включая Python, Java, JavaScript, C# или аналогичные
64	Конфигурации системы должны быть доступны для управления через веб-интерфейс, CLI и/или конфигурационные файлы
65	Система поддерживает интеграцию с внешними системами визуализации, BI, ITSM/SOAR, CMDB, threat intelligence, системами мониторинга и иными корпоративными платформами Заказчика

66	Система имеет возможность пересылать сырые, преобразованные или обогащенные события во внешние системы по Syslog TCP/UDP, raw TCP, через файл, API или аналогичный механизм
67	Система поддерживает использование публичных и/или предоставляемых производителем приложений/пакетов интеграции для популярных продуктов и сценариев безопасности
68	Система поддерживает резервирование ключевых компонентов, кластеризацию, репликацию критичных данных и отсутствие единой точки отказа при целевой архитектуре N+1
69	Система обеспечивает автоматическое восстановление, либо имеет документированную процедуру восстановления при сбоях компонентов
70	Основной режим функционирования Системы – непрерывная круглосуточная работа в автоматизированном режиме под управлением администратора
71	Система поддерживает штатный, сервисный и автономный режимы, включая возможность локальной буферизации данных при временной недоступности центральных компонентов
72	Средняя производительность по приему событий (EPS) - не менее 80 000 EPS (либо эквивалентный объем данных, рассчитанный по среднему размеру события)
73	Пиковая производительность по приему событий - не менее 150 000 EPS
74	Возможность кратковременного burst-нагрузки - до 250 000 EPS (без потери событий при корректно рассчитанной архитектуре и буферизации)
75	Суточный объем индексируемых данных - не менее 100 ГБ/сутки (с возможностью дальнейшего увеличения без смены платформы)
76	Объем хранения «горячих» данных (оперативный доступ) - не менее 180 суток
77	Объем хранения «тёплых» данных - не менее 12 месяцев
78	Общий срок хранения архивных данных - не менее 3 лет (36 месяцев)
79	Максимальная задержка обработки события до оповещения - не более 3 секунд для критичных корреляционных сценариев при штатной нагрузке
80	Потери событий при штатной нагрузке - 0% при корректной настройке источников и каналов передачи
81	Количество одновременно подключенных источников - не менее 2 000
82	Поддержка распределённых коллекторов/агентов - не менее 10 удалённых площадок
83	Количество одновременно работающих пользователей SOC - не менее 20
84	Время выполнения поискового запроса по данным за 90 суток - не более 120 секунд для согласованных типовых поисковых запросов
85	Время выполнения агрегационного отчета за 6 месяцев - не более 10 минут
86	Масштабирование производительности горизонтальное, без полной остановки системы

87	Возможность увеличения EPS минимум в 3 раза без смены архитектурного подхода
88	Поддержка раздельного хранения (hot/warm/archive tiers) обязательна
89	Отказоустойчивость - отсутствие единой точки отказа (N+1)
90	Система позволяет использовать один раз собранные и индексированные данные в различных сценариях: мониторинг ИБ, комплаенс, расследование инцидентов, выявление мошенничества, IT-операции, мониторинг приложений, цифровая аналитика и бизнес-аналитика
91	Система поддерживает расширение функциональности за счет дополнительных модулей, приложений или интеграций без необходимости миграции данных на отдельную платформу
92	Система обеспечивает возможность последующего развития в сторону автоматизации реагирования, интеграции с SOAR/ITSM и расширенной аналитики поведения пользователей и сущностей
93	Техническая поддержка решения - не менее 1 года
94	В проект включены инсталляционные и интеграционные работы
95	В проект включено проектирование
96	В проект включено сертифицированное обучение специалистов Заказчика
97	В проект включена сертификация ПО в ЦКБ
98	Язык интерфейса - русский/английский
99	В системе должно быть наличие возможности выполнять поиск, расследование, корреляцию и построение отчетности непосредственно по исходным индексированным событиям, без предварительной нормализации или загрузки данных в отдельную SQL-базу данных, рассматривается как дополнительное преимущество системы
100	Система должна иметь официально поддерживаемый производителем механизм непосредственной интеграции с Palo Alto Networks Cortex XDR, реализованный в виде штатного приложения, Add-on, модуля или иного специализированного компонента SIEM
101	Штатная интеграция должна обеспечивать автоматизированное получение из Cortex XDR взаимосвязанных данных, включающих как минимум: инциденты, alerts, детализированные события, сведения о конечных устройствах, пользователях, процессах, сетевых соединениях, объектах угроз, артефактах и статусах обработки инцидентов
102	Интеграция должна обеспечивать получение как агрегированных данных об инцидентах, так и связанных с ними детализированных событий и телеметрии, с сохранением взаимосвязи между исходным событием, alert и соответствующим инцидентом Cortex XDR
103	Полученные данные Cortex XDR должны автоматически преобразовываться средствами штатной интеграции в единую нормализованную модель данных SIEM с сохранением исходных значений и взаимосвязей между объектами

104	Нормализованные данные Cortex XDR должны непосредственно использоваться основными механизмами SIEM, включая поиск, корреляцию, аналитические правила, визуализацию, расследование инцидентов, риск-ориентированный анализ и security content, без необходимости дополнительного преобразования данных
105	Система должна обеспечивать автоматическое сопоставление данных Cortex XDR с объектами Asset и Identity, включая endpoint, IP-адрес, DNS-имя, учетную запись пользователя и иные идентификаторы, с возможностью использования данного контекста при последующем анализе
106	Данные Cortex XDR должны непосредственно участвовать в штатном механизме риск-ориентированного анализа SIEM с возможностью формирования, накопления и агрегирования риск-событий для пользователей, конечных устройств и иных объектов
107	Система должна обеспечивать автоматическое объединение событий Cortex XDR с событиями иных источников в едином аналитическом контексте на основании временных, идентификационных, сетевых и иных взаимосвязей
18	Система должна обеспечивать формирование единого инцидента или аналитического объекта на основании совокупности событий Cortex XDR и событий иных подключенных источников без необходимости создания отдельного аналитического контура для данных Cortex XDR
109	Данные Cortex XDR должны использоваться в преднастроенном security content, поставляемом производителем SIEM, включая корреляционные правила, аналитические сценарии, правила обнаружения угроз и иные механизмы анализа, без необходимости разработки Заказчиком специализированных механизмов преобразования данных Cortex XDR
110	Система должна обеспечивать сквозную связь: Cortex XDR event → нормализованное событие SIEM → Asset/Identity → Risk → Correlation → Incident с возможностью перехода между указанными объектами в рамках единого интерфейса расследования
112	При расследовании инцидента SIEM должен обеспечивать drill-down от агрегированного инцидента, корреляционного события или объекта риска до исходных данных Cortex XDR с отображением связанных endpoint, пользователя, процесса, файла, IP-адреса, домена, сетевого соединения и иных доступных атрибутов
113	Система должна обеспечивать возможность выполнения исторического поиска и ретроспективного анализа данных Cortex XDR совместно с данными иных источников без повторного получения исходных данных из Cortex XDR
114	Система должна обеспечивать применение изменённых или вновь созданных правил нормализации, классификации, обогащения и корреляции к ранее полученным данным Cortex XDR без необходимости повторной загрузки исторического массива данных
115	Данные Cortex XDR должны быть доступны для построения оперативных и исторических dashboards и аналитических представлений совместно с данными других источников с возможностью drill-down до исходного события
116	Система должна обеспечивать использование данных Cortex XDR в аналитике угроз и MITRE ATT&CK с возможностью отображения соответствующих тактик, техник и связанных событий в рамках единого расследования
117	Система должна обеспечивать контроль работоспособности штатного компонента интеграции Cortex XDR, включая контроль состояния подключения, получения данных, ошибок обработки, задержек поступления данных и признаков прекращения поступления данных
118	Для реализации требований 5.10.7–5.10.25 не допускается обязательное использование самостоятельно разработанных Заказчиком скриптов, парсеров, ETL-процедур, промежуточных баз данных либо иных программных компонентов, не входящих в штатную поддерживаемую производителем интеграцию SIEM с Cortex XDR