

№ требования	Наименование требования/ технические характеристики	Наименование участника		
		Соответствие/ Не соответствие	Ссылка на описание	Комментарии
TX-1	ПО должно поставляться сроком на 3 года (подписка, включая тех.поддержку)	Соответствие/ Не соответствие		
TX-2	Решение должно относиться к классу Extended Detection and Response (XDR)	Соответствие/ Не соответствие		
TX-3	Платформа поддерживает централизованную консоль управления с возможностью работы в режиме 24×7.	Соответствие/ Не соответствие		
TX-4	При поставке SaaS модели должны соблюдаться условия: - изоляции данных Заказчика; - размещения данных в сертифицированных дата-центрах; - использования шифрования данных при передаче и хранении.	Соответствие/ Не соответствие		
TX-5	Архитектура решения обеспечивает горизонтальное масштабирование без остановки сервисов.	Соответствие/ Не соответствие		
TX-6	Обязательно наличие следующих функций: - предотвращение эксплуатации уязвимостей; - защита от файловых и безфайловых атак; - защита от вредоносных скриптов; - детектирование и предотвращение атак типа ransomware	Соответствие/ Не соответствие		
TX-7	Наличие автоматической корреляции телеметрии из различных источников безопасности	Соответствие/ Не соответствие		
TX-8	Система обеспечивает визуализацию цепочки атаки	Соответствие/ Не соответствие		
TX-9	Решение поддерживает нативную интеграцию с сетевыми средствами защиты (межсетевые экраны, системы предотвращения вторжений)	Соответствие/ Не соответствие		
TX-10	Решение поддерживает автоматическую блокировку сетевых соединений, IP-адресов и доменов в рамках сценариев реагирования	Соответствие/ Не соответствие		
TX-11	Интеграция должна быть реализована без использования сторонних брокеров данных.	Соответствие/ Не соответствие		
TX-12	Решение обеспечивает автоматизированные сценарии реагирования на инциденты безопасности с более чем 100 готовыми плейбуками от производителя, включая: - изоляцию конечной точки; - завершение вредоносных процессов; - блокировку файлов по хэшу; - сбор форензик-артефактов.	Соответствие/ Не соответствие		
TX-13	Решение поддерживает возможность создания кастомных сценариев реагирования без написания программного кода.	Соответствие/ Не соответствие		
TX-14	Решение использует глобальные источники киберугроз, обновляемые в режиме, близком к реальному времени.	Соответствие/ Не соответствие		
TX-15	Решение поддерживает автоматическую корреляция инцидентов с актуальными индикаторами компрометации (IoC).	Соответствие/ Не соответствие		

TX-16	Решение поддерживает: - ролевую модель доступа (RBAC); - аудит действий пользователей; - хранение всей собираемой сервисной информации о событиях (телеметрии) не менее 30 дней, хранение истории инцидентов до 12 месяцев	Соответствие/ Не соответствие		
TX-17	Решение поддерживает формирование: - оперативных дашбордов; - отчётов для руководства отдела ИБ; - выгрузки данных в внешние SIEM-системы.	Соответствие/ Не соответствие		
TX-18	Решение должно поддерживать возможность контроля уязвимостей и использования сетевого сканера уязвимостей на базе промежуточного (прокси) сервера от производителя для выполнения сканирование сети и активов без установленных агентов. Решение должно поддерживать расширение в рамках единой платформы для контроля уязвимостей: - содержать алгоритмы ранжирования критичности, которые учитывают наличие защитных механизмов (активные правила предотвращения платформы обнаружения и реагирования), способных автоматически блокировать эксплуатацию конкретной уязвимости; - обеспечивать автоматический сбор данных об уязвимостях из сторонних сканеров уязвимостей и их интеграцию в единую систему управления уязвимостями; - содержать специальную панель мониторинга для визуализации наиболее критичных рисков, динамики изменения уровня риска во времени и прогресса их устранения; - обеспечивать автоматизированные встроенные плейбуки для устранения уязвимостей, включая поддержку полностью автоматизированных действий для устранения критических уязвимостей без ручного вмешательства; - предоставлять визуализацию «путей атаки», показывающую, какие уязвимости на конкретных узлах могут быть использованы для продвижения злоумышленника внутри сети; - предоставлять механизм оценки риска уязвимостей, учитывающий не только оценку CVSS, но и наличие признаков эксплуатации данной уязвимости EPSS; - возможность добавления дополнительного модуля для контроля внешней поверхности атаки и оценки внешних уязвимостей и векторов атак извне, коррелируемых с другими угрозами в рамках единой платформы; - содержать возможность автоматического сопоставления обнаруженных уязвимостей с активными инцидентами ИБ, зафиксированными на платформе обнаружения и реагирования.	Соответствие/ Не соответствие		
TX-19	Решение поддерживает интеграцию с: - Active Directory / LDAP; - с платформы поддерживающие REST API; - с внешними Syslog Receivers для отправки оповещений и логов аудита.			
TX-20	Поддерживается автоматическая синхронизация учетных записей без необходимости ручного администрирования	Соответствие/ Не соответствие		
TX-21	В решении доступно REST API	Соответствие/ Не соответствие		
TX-22	В процессе эксплуатации должен выполняться следующий функционал: - обновления сигнатур, моделей детектирования и компонентов аналитики должны выполняться автоматически, - решение должно обеспечивать непрерывную защиту при обновлении компонентов, - Вендор должен обеспечивать техническую поддержку не ниже уровня 24×7.	Соответствие/ Не соответствие		
TX-23	Решение должно поддерживать возможность удаленного подключения к конечной точке	Соответствие/ Не соответствие		
TX-24	Решение должно иметь сертификацию ISO 27001	Соответствие/ Не соответствие		

TX-25	Решение должно обладать следующими функциями по контролю устройств: - обеспечивать управление шифрованием для ОС Windows и macOS	Соответствие/ Не соответствие		
TX-26	Решение обеспечивает стабильную обработку телеметрии от: - не менее 10 000 конечных точек в рамках одного логического тенанта; - с возможностью последующего масштабирования без изменения архитектуры.	Соответствие/ Не соответствие		
TX-27	Решение должно поддерживать возможность контроля передачи данных в LLM и облачные хранилища и предотвращения утечек данных на конечных точках в рамках единой платформы управления угрозами и единого агента, устанавливаемого на конечные точки.	Соответствие/ Не соответствие		
TX-28	Агент конечной точки не должен потреблять в среднем более: - 5% CPU в штатном режиме; - 500 МБ оперативной памяти; - 1 Гб дискового пространства.	Соответствие/ Не соответствие		
TX-29	Решение должно обеспечивать отказоустойчивость компонентов аналитики и управления без потери данных и телеметрии.	Соответствие/ Не соответствие		
TX-30	Решение должно поддерживать возможность применения специального модуля для выявления и удаления фишинговых писем за счет продвинутого анализа содержимого при помощи AI на предмет намерений, содержащихся в письме	Соответствие/ Не соответствие		
TX-31	Интеграция должна обеспечивать: - получение информации о пользователях, группах и ролях; - корреляцию событий безопасности с учетными записями пользователей; - использование данных каталогов для построения контекста инцидентов.	Соответствие/ Не соответствие		
TX-32	Обеспечивается двустороннюю интеграцию с внешними SIEM-системами, включая: - передачу инцидентов и алертов; - передачу обогащённых событий.	Соответствие/ Не соответствие		
TX-33	Поддержка интеграции через: - REST API; - Syslog; - нативные коннекторы.	Соответствие/ Не соответствие		
TX-34	Решение возможно использовать в качестве: - источника событий для SIEM; - автономной XDR-платформы без обязательного подключения SIEM.	Соответствие/ Не соответствие		
TX-35	Интеграция должна обеспечивать: - получение телеметрии безопасности; - выявление фишинговых атак и компрометации учетных записей.	Соответствие/ Не соответствие		
TX-36	Решение должно предоставлять публичный, документированный REST API для: - получения событий и инцидентов; - управления объектами защиты; - запуска сценариев реагирования.	Соответствие/ Не соответствие		
TX-37	API поддерживает: - аутентификацию по токенам; - разграничение прав доступа; - журналирование обращений.	Соответствие/ Не соответствие		

TX-38	Решение должно поддерживать интеграцию с системами класса ITSM для: - автоматического создания инцидентов; - передачи статусов расследования; - закрытия инцидентов по результатам реагирования.	Соответствие/ Не соответствие		
TX-39	Должна поддерживаться возможность использования интеграций в рамках: - автоматических playbook-ов; - полуавтоматических сценариев реагирования.	Соответствие/ Не соответствие		
TX-40	Лицензирование решения должно осуществляться по количеству защищаемых конечных точек с возможностью гибкого увеличения лицензируемого объема	Соответствие/ Не соответствие		
TX-41	В стоимость лицензии должны быть включены: - функции предотвращения атак на конечных точках; - функции обнаружения и реагирования (EDR/XDR); - централизованная консоль управления; - аналитика на основе машинного обучения и поведенческих моделей; - встроенные сценарии автоматического реагирования.	Соответствие/ Не соответствие		
TX-42	Дополнительная оплата не допускается за следующий функционал: - корреляцию инцидентов.	Соответствие/ Не соответствие		
TX-43	Лицензия должна включать право использования решения: - в круглосуточном режиме; - без ограничений на количество инцидентов и событий	Соответствие/ Не соответствие		
TX-44	В рамках лицензии должно предоставляться: - регулярное обновление сигнатур; - обновление аналитических моделей; - обновление функциональных компонентов платформы.	Соответствие/ Не соответствие		
TX-45	Лицензия должна включать: - техническую поддержку уровня 24x7; - доступ к базе знаний и рекомендациям по реагированию.	Соответствие/ Не соответствие		
TX-46	Лицензирование не должно зависеть от: - объема обрабатываемого трафика; - количества аналитических правил; - числа пользователей консоли управления.	Соответствие/ Не соответствие		
TX-47	Требования к режимам функционирования Системы Основной режим функционирования Системы – автоматизированный, под управлением администратора. Система должна обеспечивать возможность работы в следующих режимах: - штатный режим (непрерывная круглосуточная работа); - автономный режим (в случае отсутствия связи между компонентами системы или с внешними сетями).	Соответствие/ Не соответствие		
TX-48	Требования к численности и квалификации персонала Исполнителя, для обеспечения поставки программного комплекса и запуска рабочего функционирования системы: - в составе персонала Исполнителя должны присутствовать минимум одна штатная единица инженера технической поддержки; - инженер технической поддержки должен обладать знаниями в объеме, необходимом для выполнения штатного технического и аварийного обслуживания Системы у Заказчика.	Соответствие/ Не соответствие		

TX-49	<p>Требования к аудиту, мониторингу и отчетности</p> <ul style="list-style-type: none"> <li>- система должна обеспечивать аудит действий пользователей и администраторов, регистрацию событий безопасности и эксплуатации, а также мониторинг состояния и доступности компонентов;</li> <li>- система должна иметь поддержку аудита в реальном времени с возможностью отправки оповещений при выявлении подозрительной активности;</li> <li>- все события должны фиксироваться с указанием даты и времени, источника и результата действия;</li> <li>- система должна быть обеспечена защита журналов от несанкционированного изменения и удаления;</li> <li>- отчёты должны быть доступны по запросу и/или по расписанию, с возможностью экспорта в стандартные форматы (PDF, CSV).</li> <li>- срок хранения аудиторских и мониторинговых данных (логов) – не менее 12 месяцев</li> </ul>	Соответствие/ Не соответствие		
TX-50	Количество защищаемых конечных точек – не менее 2000	Соответствие/ Не соответствие		
TX-51	В проект включены инсталляционные работы	Соответствие/ Не соответствие		
TX-52	В проект включено проектирование	Соответствие/ Не соответствие		
TX-53	В проект включено обучение специалистов Заказчика	Соответствие/ Не соответствие		
TX-54	В проект включена сертификация ПО в ЦКБ	Соответствие/ Не соответствие		
TX-55	Наличие у Исполнителя МАФ	Соответствие/ Не соответствие		

Дата: 03.06.2026

дд/мм/гггг 03.06.2026

Составил:

Начальник отдела ИБ

Должность



Абдульваат Р.А.

ФИО

Согласовано:

Директор Департамента ДИБиР

Должность



Олматов Б.А.

ФИО