Приложение №2 к Техническому заданию "Система управления информацией и событиями безопасности (SIEM) "

№ требования	Наименование требования/ технические характеристики	Тип критерия
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)	Блокирующий
2	ПО (решение) должно относится к классу SIEM (Security Information and Event Management)	Блокирующий
3	Система должна предоставлять единый интерфейс и единое хранилище данных для задач логгирования, мониторинга безопасности, расследования инцидентов, отчетности, визуализации и администрирования.	Блокирующий
4	Система должна обеспечивать сохранение исходных данных с возможностью последующего поиска и анализа, при этом предварительная нормализация не должна быть обязательным условием приема данных	Блокирующий
5	Система должна обеспечивать работу с разнородными машинными данными без необходимости предварительного преобразования всех источников в единую реляционную модель	Блокирующий
6	Решение должно иметь подтвержденную практику промышленного применения у крупных корпоративных заказчиков и развитую экосистему документации, профессиональных сервисов, обучения, поддержки и партнеров	Блокирующий
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	Блокирующий
8	Архитектура решения поддерживает горизонтальное масштабирование компонентов сбора, индексирования/хранения и поиска без полной переустановки системы	Блокирующий
9	Система обеспечивает распределенный поиск по нескольким узлам хранения/индексации и поддерживать параллельную обработку поисковых запросов	Блокирующий
10	Система поддерживает размещение разных типов данных в отдельных логических хранилищах для оптимизации производительности поиска, разграничения доступа и управления сроками хранения	Блокирующий
11	Система поддерживает обработку крупных объемов машинных данных и иметь документально подтвержденную возможность масштабирования до десятков ТБ данных в сутки при соответствующем проектировании инфраструктуры	Блокирующий
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.	Блокирующий
13	Агентское ПО поддерживает шифрование передачи данных, кэширование при недоступности центральных компонентов, балансировку нагрузки между принимающими узлами и передачу данных по надежному транспортному протоколу	Блокирующий
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	Блокирующий
15	Система поддерживает индексирование многострочных и сложных событий без потери структуры события и исходной временной метки	Блокирующий
16	Система не должна требовать предварительного описания структуры каждого источника до начала приема данных	Блокирующий
17	Система должна обеспечивать прием, индексирование и хранение исходных, немодифицированных машинных данных из любых источников	Блокирующий
18	Система корректно обрабатывает временные метки из разных часовых поясов и сохранять оригинальное время события наряду со временем поступления в Систему	Блокирующий
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	Блокирующий
20	Поддерживаться автоматическая проверка доступности источников, контроль полноты поступающих событий и оповещение при прекращении поступления данных от критичных источников.	Блокирующий
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	Блокирующий
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	Блокирующий
23	В Системе присутствует возможность хранения оперативных, теплых и архивных данных с гибкой настройкой сроков хранения по типам источников, индексам, критичности и требованиям комплаенса	Блокирующий
24	Система поддерживает детализированное управление данными по мере их устаревания: перенос на более дешевое/внешнее хранилище, архивирование и/или удаление согласно политикам Заказчика	Блокирующий
25	Система поддерживает репликацию данных/индексов для обеспечения доступности, целостности, устойчивости к сбоям и повышения производительности поиска	Блокирующий
26	Существует возможность масштабирования хранилища без остановки всей Системы	Блокирующий
27	Существует защита журналов и аудиторских данных от несанкционированного изменения и удаления, включая механизмы проверки целостности	Блокирующий
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	Блокирующий
29	Изменение логики извлечения полей, справочников, правил нормализации или обогащения не требует обязательной повторной загрузки ранее сохраненных событий	Блокирующий
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)	Блокирующий
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	Блокирующий
32	Поддерживаются корреляция нескольких учетных записей/логинов с одним сотрудником или субъектом	Блокирующий
33	Поддерживается интеграция с базами активов (CMDB) для получения информации об устройствах: hostname, IP, MAC, местоположение, владелец, критичность, наличие чувствительных данных, соответствие регуляторным требованиям	Блокирующий
34	Система позволяет применять новые справочники и контекстные данные к ранее проиндексированным событиям для поиска и отчетности за прошлые периоды	Блокирующий
35	Система поддерживает интерактивный полнотекстовый поиск по любому полю индексированных данных с использованием ключевых слов, временных интервалов, логических операторов, регулярных выражений и подстановочных символов	Блокирующий
36	Система поддерживает как поиски в реальном времени, так и запланированные поиски, а также параллельное выполнение нескольких поисковых запросов	Блокирующий
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	Блокирующий
38	Система позволяет сохранять, редактировать, повторно использовать и передавать поисковые запросы другим пользователям с учетом ролевой модели доступа	Блокирующий
39	Система поддерживает статистический анализ: подсчет, уникальные значения, сумма, минимум, максимум, среднее, медиана, мода, стандартное отклонение, дисперсия, перцентили, первое/последнее появление значения	Блокирующий
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	Блокирующий
41	Система поддерживает корреляцию событий по временным, логическим, поведенческим и статистическим правилам, включая многошаговые сценарии атак	Блокирующий
42	Система поддерживает использование моделей kill chain, MITRE ATT&CK или аналогичных фреймворков для классификации и описания сценариев выявления	Блокирующий

43	Система позволяет создавать собственные правила корреляции, изменять существующие правила и тестировать их до ввода в промышленную эксплуатацию	Блокирующий
44	Система предоставляет преднастроенный SIEM-контент: корреляционные правила, дашборды, отчеты, модели данных, сценарии расследования и шаблоны мониторинга безопасности с возможностью адаптации под инфраструктуру Заказчика	Блокирующий
45	Система поддерживает мониторинг в режиме, близком к реальному времени, и формирование оповещений по результатам поисков, корреляционных правил и аналитических сценариев	Блокирующий
46	Оповещения поддерживают настройку приоритетов, подавление повторных срабатываний, ограничение частоты срабатывания и маршрутизацию ответственным группам	Блокирующий
47	Система поддерживает отправку уведомлений по электронной почте, через интеграции с внешними системами, Webhook/API, запуск пользовательских скриптов либо иные механизмы автоматизации	Блокирующий
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	Блокирующий
49	Система обеспечивает переход от сводного события/дашборда/корреляционного срабатывания к исходным событиям для детального расследования	Блокирующий
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	Блокирующий
51	Визуализации поддерживают обновление в реальном времени, drill-down от агрегированных показателей к исходным событиям и выделение аномалий/выбросов	Блокирующий
52	Система позволяет создавать отчеты и дашборды как техническим, так и нетехническим пользователям, включая визуальное редактирование панелей и настройку заголовков, легенд, осей и фильтров	Блокирующий
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	Блокирующий
54	Система поддерживает отчеты и панели мониторинга для задач соответствия требованиям ИБ и регуляторики, включая ISO 27002, NIST, PCI DSS и аналогичные стандарты	Блокирующий
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	Блокирующий
56	Система поддерживает интеграцию с Active Directory/LDAP и корпоративными системами единого входа (SSO)	Блокирующий
57	Передача данных между компонентами осуществляется по защищенным каналам с использованием современных криптографических протоколов	Блокирующий
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	Блокирующий
59	Аудиторские события Системы содержат дату и время, пользователя/субъект, источник, выполненное действие и результат выполнения	Блокирующий
60	Система поддерживает механизмы подтверждения целостности индексированных событий, включая хеширование и/или цифровую подпись событий либо функционально эквивалентный механизм контроля подлинности	Блокирующий
61	Система обеспечивает мониторинг собственной конфигурации, доступности компонентов и состояния системных сервисов с возможностью оповещения	Блокирующий
62	Система предоставляет открытые интерфейсы API для доступа к индексированным данным, выполнения поисковых запросов, управления объектами конфигурации и интеграции с внешними системами	Блокирующий
63	Система должна поддерживать SDK или иметь библиотеки для распространенных языков программирования, включая Python, Java, JavaScript, C# или аналогичные	Блокирующий
64	Конфигурации системы должны быть доступны для управления через веб-интерфейс, CLI и/или конфигурационные файлы	Блокирующий
65	Система поддерживает интеграцию с внешними системами визуализации, BI, ITSM/SOAR, CMDB, threat intelligence, системами мониторинга и иными корпоративными платформами Заказчика	Блокирующий
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	Блокирующий
67	Система поддерживает использование публичных и/или предоставляемых производителем приложений/пакетов интеграции для популярных продуктов и сценариев безопасности	Блокирующий
68	Система поддерживает резервирование ключевых компонентов, кластеризацию, репликацию критичных данных и отсутствие единой точки отказа при целевой архитектуре N+1	Блокирующий
69	Система обеспечивает автоматическое восстановление, либо имеет документированную процедуру восстановления при сбоях компонентов	Блокирующий
70	Основной режим функционирования Системы – непрерывная круглосуточная работа в автоматизированном режиме под управлением администратора	Блокирующий
71	Система поддерживает штатный, сервисный и автономный режимы, включая возможность локальной буферизации данных при временной недоступности центральных компонентов	Блокирующий
72	Средняя производительность по приему событий (EPS) - не менее 80 000 EPS (либо эквивалентный объем данных, рассчитанный по среднему размеру события)	Блокирующий
73	Пиковая производительность по приему событий - не менее 150 000 EPS	Блокирующий
74	Возможность кратковременного burst-нагрузки - до 250 000 EPS (без потери событий при корректно рассчитанной архитектуре и буферизации)	Блокирующий
75	Суточный объем индексируемых данных - не менее 100 ГБ/сутки (с возможностью дальнейшего увеличения без смены платформы)	Блокирующий
76	Объем хранения «горячих» данных (оперативный доступ) - не менее 180 суток	Блокирующий
77	Объем хранения «тёплых» данных - не менее 12 месяцев	Блокирующий
78	Общий срок хранения архивных данных - не менее 3 лет (36 месяцев)	Блокирующий
79	Максимальная задержка обработки события до оповещения - не более 3 секунд для критичных корреляционных сценариев при штатной нагрузке	Блокирующий
80	Потери событий при штатной нагрузке - 0% при корректной настройке источников и каналов передачи	Блокирующий
81	Количество одновременно подключенных источников - не менее 2 000	Блокирующий
82	Поддержка распределённых коллекторов/агентов - не менее 10 удалённых площадок	Блокирующий
83	Количество одновременно работающих пользователей SOC - не менее 20	Блокирующий
84	Время выполнения поискового запроса по данным за 90 суток - не более 120 секунд для согласованных типовых поисковых запросов	Блокирующий
85	Время выполнения агрегационного отчета за 6 месяцев - не более 10 минут	Блокирующий
86	Масштабирование производительности горизонтальное, без полной остановки системы	Блокирующий
87	Возможность увеличения EPS минимум в 3 раза без смены архитектурного подхода	Блокирующий

88	Поддержка раздельного хранения (hot/warm/archive tiers) обязательна	Блокирующий
89	Отказоустойчивость - отсутствие единой точки отказа (N+1)	Блокирующий
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	Блокирующий
91	Система поддерживает расширение функциональности за счет дополнительных модулей, приложений или интеграций без необходимости миграции данных на отдельную платформу	Блокирующий
92	Система обеспечивает возможность последующего развития в сторону автоматизации реагирования, интеграции с SOAR/ITSM и расширенной аналитики поведения пользователей и сущностей	Блокирующий
93	Гарантийная поддержка решения - не менее 1 года	Блокирующий
94	В проект включены инсталляционные и интеграционные работы	Блокирующий
95	В проект включено проектирование	Блокирующий
96	В проект включено сертифицированное обучение специалистов Заказчика	Блокирующий
97	В проект включена сертификация ПО в ЦКБ	Блокирующий
98	Язык интефейса - русский/английский	Блокирующий
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	Не блокирующий
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	Не блокирующий
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	Не блокирующий
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	Не блокирующий
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	Не блокирующий
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	Не блокирующий
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	Не блокирующий
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	Не блокирующий
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	Не блокирующий
108	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	Не блокирующий
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	Не блокирующий
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	Не блокирующий
111	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	Не блокирующий
112	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	Не блокирующий
113	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	Не блокирующий
114	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	Не блокирующий
115	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	Не блокирующий
116	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	Не блокирующий
117	Для реализации пунктов 99-118 SoC 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	Не блокирующий
118	Все указанные механизмы интеграции SIEM и XDR 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	Не блокирующий

Дата: дд/мм/гггг

Составил:
Начальник отдела ИБ — Абдульваат Р.А.
Должность — ФИО

Согласовано:
Директор Департамента ДИБиР — Олматов Б.А.
Должность — ФИО