“O‘ZBEKISTON SANOAT-QURILISH BANKI” AKSIYADORLIK TIJORAT BANKI
АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНК “УЗБЕКСКИЙ ПРОМЫШЛЕННО-СТРОИТЕЛЬНЫЙ БАНК

TEXNIK TOPSHIRIQNOMA

№ 1423
2025 yil «20» «mart»

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Комплексная система сбора, анализа и координации событий ИТ и ИБ инфраструктуры банка.

Ташкент 2025 г.

1. Полное наименование и условное обозначение

Целью закупки является внедрение комплексной системы сбора, анализа и координации событий ИТ и ИБ инфраструктуры банка (далее – Система), обеспечивающей централизованное управление событиями, мониторинг цифровых активов и автоматизацию реагирования на инциденты.

2. Наименование организаций заказчика и исполнителя

Заказчик – АКБ «Узпромстройбанк»

Адрес «Заказчика»: Республика Узбекистан, г.Ташкент, 100000, Юнусабадский район, ул. Шахрисабзская, дом №3; Тел.: (998-78) 777 77 55 (7054)

МФО: 00440; ИНН: 200 833 707;

Наименование банка: ОПЕРУ при АКБ «Узпромстройбанк»

Адрес электронной почты: info@sqb.uz;

Исполнитель по данному проекту будет определен на основе результатов отбора.

Исполнитель должен отвечать следующим требованиям:

- Наличие сертифицированных сотрудников по предлагаемым продуктам (не менее 2 сотрудников)
- Авторизация от производителя программного обеспечения с указанием полномочий продавать продукты и услуги на территории Республики Узбекистан.
- Предоставить гарантийное письмо от правообладателя (правообладателей) о том, что предлагаемые программные продукты будут покрыты технической поддержкой и гарантией со стороны правообладателя в срок на 3 года с момента передачи лицензионных ключей
- Предоставить гарантийное письмо от правообладателя (правообладателей) о том, что в рамках внедрения со стороны правообладателя для работы с сотрудниками заказчика будет предоставлен выделенный сотрудник для работы по всем организационным и техническим вопросам, связанным с процессом внедрения.
- Предоставить гарантийное письмо от правообладателя (правообладателей) о том, что в рамках оказания технической поддержки на программные продукты со стороны правообладателя для работы с сотрудниками заказчика будет предоставлен выделенный сотрудник для работы по всем сервисным заявкам.
- Внедрение всех предлагаемых систем на условиях «под ключ» и поддержка в течение срока действия гарантии (гарантийное письмо).

3. Плановые сроки начала и окончания работ

Срок начала: подписание договора/контракта;

Срок окончания: 2 месяца.

4. Комплексная система сбора, анализа и координации событий ИТ и ИБ инфраструктуры банка.

Комплексная Система должна содержать обязательные модули:

1. Программно-аппаратный комплекс сбора, нормализации, аналитики событий и инцидентов инфраструктуры банка – предназначен для централизованного сбора, хранения, нормализации и анализа событий, поступающих из различных источников (серверов, сетевого

оборудования, баз данных, приложений и систем безопасности). Обеспечивает выявление инцидентов, построение отчетности и анализ корреляции событий.

2. Программно-аппаратный комплекс сбора, мониторинга и анализа данных сетевого трафика – предназначен для анализа сетевого взаимодействия, выявления аномальной активности и возможных угроз, поступающих из внешней или внутренней сети. Обеспечивает сбор и обработку данных о сетевых соединениях, контроль трафика и выявление подозрительных активностей.

3. Программно-аппаратный комплекс наблюдения и контроля состояния и производительности цифровых активов банка – отвечает за мониторинг работоспособности и загрузки ИТ-инфраструктуры, включая серверы, виртуальные машины, сети, базы данных и приложения. Обеспечивает контроль доступности и производительности ключевых систем банка, формирует оповещения о нарушениях и сбоях.

4. Программно-аппаратный комплекс координации инцидентов ИТ и ИБ – обеспечивает автоматизацию реагирования на выявленные инциденты, позволяет настраивать сценарии обработки событий, интегрируется с другими системами управления безопасностью и инцидентами. Предоставляет функционал по управлению процессами расследования инцидентов, назначению ответственных и документированию действий по их устранению.

Комплексная Система должна поддерживать работу ИТ и ИБ-служб банка, обеспечивать оперативное выявление угроз и аномалий, автоматизировать процессы реагирования и повышать устойчивость ИТ-инфраструктуры.

5. Требования к программно-аппаратному комплексу сбора, нормализации, аналитики событий и инцидентов инфраструктуры банка

№	Требование	Соответствие
1.1.	Иметь форм-фактор для установки в стандартную серверную стойку и иметь высоту	Не более 2RU
1.2.	Иметь установленных процессоров серии не ниже Gold, каждый из которых должен иметь не менее 24 (двадцати четырёх) ядер, работающих на частоте не ниже 3.0 ГГц, поддерживать работу памяти с частотой не менее 2933 МГц, иметь кэш-память объёмом не менее 35 Мбайт. Максимальная рассеиваемая мощность процессора должна быть не более 210 Ватт. Должна быть реализована возможность работы с 64х разрядными приложениями на аппаратном уровне.	Не менее 2
1.3.	Наличие слотов DDR для установки модулей памяти	Не менее 24
1.4.	Должно быть установлено модулей памяти RDIMM объёмом не менее 32ГБ каждый, поддерживающих работу на частоте не менее 3200 МГц	Не менее 16
1.5.	Поддерживать установку жёстких дисков форм-фактора не более 2.5’	Не менее 8
1.6.	Иметь установленных сетевых адаптеров с не менее чем с 2 (двумя) портами 10GBase-T	Не менее 2
1.7.	Иметь на каждом сервере установленных драйвов (устройств) SAS SSD объёмом не менее 1.92 ТБ каждый	Не менее 8
1.8.	Иметь блоков питания мощностью не менее 1600 Вт каждый, с	Не менее 2

№	Требование	Соответствие
	возможностью горячей замены; поддержка резервирования питания; кабели питания C13-C14 должны входить в комплект поставки	
1.9.	Дополнительно в комплект поставки должны входить кабели питания типа Euro с длиной	Не менее 3 м
1.10.	Сервер должен быть укомплектован полным комплектом отказоустойчивых резервированных вентиляторов охлаждения	Обязательно
1.11.	Должен быть совместим как минимум со следующими операционными системами и гипервизорами:	Vmware версии не ниже 7
1.12.	Сервер должен быть укомплектован отдельным независимым портом управления 100/1000 Мбит Ethetnet	Обязательно
1.13.	Сервер должен быть укомплектован монтажными рельсами для установки сервера в стандартную телекоммуникационную стойку 19’’	Обязательно
1.14.	Сервер должен быть укомплектован TPM модулем безопасности	Обязательно
1.15.	Должен иметь встроенные аппаратно-программные средства в комплекте с необходимыми для мониторинга и управления лицензиями для удалённого управления и мониторинга (включая выделенный порт управления)	Обязательно
1.16.	Гарантийный срок на оборудования должен быть не менее 3 лет	Обязательно
1.17.	Программный модуль должен предоставляться в виде виртуального программного обеспечения или программного обеспечения на Linux для установки на программно-аппаратный комплекс и функционировать в режиме постоянной лицензии с поддержкой сроком на 3 года.	Обязательно
1.18.	Программный модуль должен функционировать на базе операционной системы Linux.	Обязательно
1.19.	Программный модуль должен обеспечивать централизованный сбор и управление логами из ИТ-инфраструктуры банка. Производительность Модуля должна быть не меньше 5000 событий в секунду.	Обязательно
1.20.	Программный модуль должен работать в режиме, максимально приближенном к реальному времени, обеспечивая оперативную обработку событий.	Обязательно
1.21.	Программный модуль должен обеспечивать полноценное функционирование без доступа к сети Интернет, если это требуется политиками безопасности банка.	Обязательно
1.22.	Программный модуль должен поддерживать возможность развертывания независимых инстансов в филиалах банка с возможностью централизованного доступа к данным.	Обязательно
1.23.	Инстансы Модуля должны сохранять работоспособность в случае потери связи с центральным узлом, обеспечивая непрерывность мониторинга.	Обязательно
1.24.	Программный модуль должен обеспечивать эффективную обработку до 100 ГБ данных в сутки.	Обязательно

№	Требование	Соответствие
1.25.	Программный модуль должен поддерживать хранение логов (ретенцию данных) не менее 180 дней, в зависимости от требований банка.	Обязательно
1.26.	Программный модуль не должен ограничивать количество зарегистрированных пользователей, а также число одновременно работающих пользователей.	Обязательно
1.27.	Лицензия на Программный модуль не должна ограничивать количество источников данных, из которых поступают журналы и события.	Обязательно
1.28.	Архитектура Модуля должна предусматривать разделение ролей между отдельными компонентами (серверы/виртуальные машины). Минимально должны быть выделены три типа ролей: Агрегация (сбор и обработка данных), Презентация (визуализация и аналитика), Ретенция (хранение и управление логами).	Обязательно
1.29.	Программный модуль должен поддерживать добавление новых узлов для обработки, визуализации или хранения данных, что позволяет масштабировать производительность. Такое расширение должно выполняться без необходимости перезапуска работающего Модуля.	Обязательно
1.30.	Программный модуль должен разрабатываться в соответствии с рекомендациями OWASP Testing Guide, включая соблюдение требований OWASP Top 10.	Обязательно
1.31.	Программный модуль должен соответствовать требованиям OWASP ASVS (Application Security Verification Standard) версии 4.0 как минимум на уровне L1.	Обязательно
1.32.	Программный модуль должен обеспечивать полный аудит активности пользователей, включая: успешные/неуспешные попытки входа в Программный модуль, полную историю выполненных операций, фиксацию выполненных запросов, контроль изменений уровней доступа пользователей.	Обязательно
1.33.	Программный модуль должен поддерживать возможность ручного задания уровня детализации собираемых данных аудита.	Обязательно
1.34.	Программный модуль должен быть основан на современной нереляционной базе данных типа NoSQL.	Обязательно
1.35.	Программный модуль должен поддерживать мультитенантную архитектуру.	Обязательно
1.36.	Программный модуль должен позволять создание парсеров через графический интерфейс (GUI).	Обязательно
1.37.	Программный модуль должен поддерживать возможность предсказательного анализа данных на основе исторических данных, накопленных в Модуле.	Обязательно
1.38.	Программный модуль должен обеспечивать построение прогностических моделей с использованием математических и статистических методов (Machine Learning).	Обязательно
1.39.	Программный модуль должен быть оснащен механизмами интеллектуального анализа данных на основе алгоритмов искусственного интеллекта (AI).	Обязательно

№	Требование	Соответствие
1.40.	Алгоритмы AI должны обеспечивать предсказание поведения Модуля, анализируя объем событий и числовые показатели в них, такие как: переданные байты (sent_bytes), размер файлов (file_size), длительность сессий (session_duration).	Обязательно
1.41.	Алгоритмы AI должны помогать администраторам Модуля выявлять аномалии в данных, анализируя: отдельные числовые параметры, множество числовых параметров, текстовые данные, смешанные данные.	Обязательно
1.42.	Выявление аномалий должно включать систему скоринга, что позволит операторам сосредотачиваться на наиболее критических событиях.	Обязательно
1.43.	Программный модуль должен поддерживать ненадзорное (unsupervised) динамическое группирование событий на основе их характеристик.	Обязательно
1.44.	Программный модуль должен предоставлять возможность графической визуализации сгруппированных событий, позволяющая легко идентифицировать изолированные инциденты.	Обязательно
1.45.	Программный модуль должен позволять создание детекционных правил для быстрого реагирования на выявленные аномалии.	Обязательно
1.46.	Программный модуль должен обеспечивать визуализацию данных в различных формах, включая: оригинальные журналы событий (raw logs), списки, таблицы, графики, диаграммы, дашборды и т. д.	Обязательно
1.47.	Программный модуль должен поддерживать визуализацию как текстовых, так и числовых значений, содержащихся в логах.	Обязательно
1.48.	Программный модуль должен поддерживать экспорт данных о событиях и инцидентах в форматы CSV и HTML для последующего анализа, включая анализ результатов работы корреляционных правил.	Обязательно
1.49.	Программный модуль должен обеспечивать разбор (парсинг) входящих сообщений в следующих форматах: - Syslog - WEF (Windows Event Forwarding) - Flat file (плоские файлы логов) - Event log (журналы событий Windows) - WMI (Windows Management Instrumentation) - SNMP trap (перехват SNMP-трапов) - XML - JSON - JDBC/ODBC (доступ к базам данных) - CSV (значения, разделенные запятыми) - Email (анализ почтовых сообщений)	Обязательно
1.50.	Программный модуль должен поддерживать возможность добавления новых форматов логов по запросу банка, если возникает необходимость в интеграции с дополнительными источниками данных.	Обязательно
1.51.	Программный модуль должен обеспечивать сбор логов из облачных	Обязательно

№	Требование	Соответствие
	сред, включая AWS и Microsoft Azure.	
1.52.	Программный модуль должен поддерживать сбор данных из различных типов баз данных, включая: - Реляционные БД: MSSQL, Oracle, PostgreSQL, SQL Server - NoSQL-БД: MongoDB, Apache Cassandra - БД реального времени: InfluxDB, Apache Kafka	Обязательно
1.53.	Программный модуль должен предоставлять возможность отображения логов в их исходном виде (RAW-данные) в пользовательском интерфейсе до их парсинга.	Обязательно
1.54.	Программный модуль должен поддерживать как агентский (с использованием агентов), так и безагентский сбор событий.	Обязательно
1.55.	Все операции с записями в базе данных должны выполняться только с использованием JSON через документированное API.	Обязательно
1.56.	Доступ к данным базы должен осуществляться через REST API, без использования SQL-клиентов.	Обязательно
1.57.	Программный модуль должен поддерживать создание кастомных парсеров для нестандартных форматов логов, используя регулярные выражения и стандартизированные форматы данных.	Обязательно
1.58.	Интерфейс Модуля должен поддерживать парсинг по условиям, с выбором оптимального метода разборки данных (например, REGEX, JSON, XML) и возможностью подключения разных парсеров в зависимости от значений полей.	Обязательно
1.59.	Программный модуль должен включать предопределенный набор парсеров событий, позволяющий анализировать распространенные типы логов без дополнительной настройки.	Обязательно
1.60.	Программный модуль должен позволять нормализацию сообщений путем изменения значений полей и их обогащения дополнительными данными, основанными на сопоставлении с известными шаблонами.	Обязательно
1.61.	Программный модуль должен поддерживать поиск данных с фильтрацией по полям, полученным после парсинга.	Обязательно
1.62.	Программный модуль должен позволять обогащение логов математическими операциями, выполняемыми на основе данных из других полей.	Обязательно
1.63.	Программный модуль должен поддерживать анонимизацию входных данных, скрывая чувствительную информацию, которая не должна храниться в Модуле или может нарушать внутренние политики безопасности банка.	Обязательно
1.64.	Программный модуль должен поддерживать работу как с однострочными (single-line), так и многострочными (multi-line) логами.	Обязательно
1.65.	Программный модуль должен распознавать различные форматы времени и даты и приводить их к единому стандарту.	Обязательно
1.66.	Программный модуль должен включать встроенный компонент для создания электронной документации, который позволяет автоматически или вручную добавлять контент, используя данные, собранные Модулем.	Обязательно

№	Требование	Соответствие
1.67.	Компонент электронной документации должен поддерживать возможность создания и добавления диаграмм архитектуры ИТ-инфраструктуры, таблиц и списков.	Обязательно
1.68.	Программный модуль должен поддерживать объединение результатов двух независимых запросов в едином ответе, без использования SQL-запросов.	Обязательно
1.69.	Программный модуль должен обеспечивать возможность редактирования значений в собранных данных через интерфейс.	Обязательно
1.70.	Инцидент, сформированный в результате корреляции, должен быть доступен через стандартный поисковый механизм, предоставляемый Модулем.	Обязательно
1.71.	Программный модуль должен позволять использование зафиксированных инцидентов для создания новых корреляционных правил и генерации уведомлений или тревожных событий.	Обязательно
1.72.	Программный модуль должен поддерживать построение запросов с использованием SQL и Piped Processing Language (PPL).	Обязательно
1.73.	Программный модуль должен обеспечивать корреляцию событий в режиме реального времени.	Обязательно
1.74.	Программный модуль должен поддерживать возможность создания новых корреляционных правил, а также модификацию существующих.	Обязательно
1.75.	Программный модуль должен обеспечивать возможность создания кастомных корреляционных правил, основанных на обнаружении определенных событий, включая: - Обнаружение конкретного содержимого в логах. - Обнаружение значений поля, присутствующих в заданном списке. - Обнаружение значений поля, отсутствующих в заданном списке. - Обнаружение изменений значений одного из нескольких полей. - Обнаружение событий, происходящих с заданной частотой. - Обнаружение событий, частота которых изменяется по сравнению с предыдущими временными периодами. - Обнаружение пропажи сообщений (непоступление ожидаемых логов). - Обнаружение новых значений в определенных полях в заданном временном интервале. - Обнаружение инцидентов, возникающих в результате последовательности событий.	Обязательно
1.76.	Программный модуль должен поддерживать возможность создания пользовательских алгоритмов оценки инцидентов.	Обязательно
1.77.	Корреляционные правила и алгоритмы оценки инцидентов должны быть доступны для создания и модификации как через GUI, так и через API.	Обязательно
1.78.	Программный модуль должен поддерживать настройку временного окна и условий для событий, подлежащих корреляции.	Обязательно

№	Требование	Соответствие
1.79.	Программный модуль должен позволять выполнение запросов по всей истории накопленных данных.	Обязательно
1.80.	Обработка инцидентов и автоматизация: - Программный модуль должен поддерживать механизмы управления инцидентами и обмена информацией между операторами, включая назначение инцидентов операторам и изменение их статуса. - Программный модуль должен обеспечивать функционал сценариев обработки инцидентов (Playbooks). - Программный модуль должен автоматически предлагать соответствующие сценарии реагирования на инциденты. - Сценарии обработки инцидентов должны поддерживать их симуляцию и тестирование, включая проверку на тестовом ИТ-ресурсе. - Программный модуль должен обеспечивать возможность создания и редактирования пользовательских сценариев обработки инцидентов. - Программный модуль должен поддерживать уведомления о инцидентах, включая отправку сообщений в другие системы или пользователям (Email, Telegram, Jira, Microsoft Teams, Google Chat и другие). - Программный модуль должен поддерживать тестирование корреляционных правил и предупреждений перед их внедрением, при этом тестовые срабатывания не должны создавать реальные инциденты. - Программный модуль должен поддерживать автоматическое оценивание рисков на основе настраиваемых критериев. - Программный модуль должен обеспечивать категоризацию объектов (IP-адреса, учетные записи и другие параметры) с учетом веса риска. - Программный модуль должен поддерживать автоматизированное выполнение задач на мониторируемых системах в случае обнаружения угрозы, соответствующей заданным правилам. - Создаваемые инциденты должны иметь встроенный уровень критичности, с возможностью изменения уровня критичности для каждого правила.	Обязательно
1.81.	Документация и лицензирование: - Система должна включать встроенный GUI-Программный модуль для создания и редактирования электронной документации, который дополняет данные, собранные системой. - Система должна поддерживать приобретение бессрочных лицензий с поддержкой производителя - Лицензия не должна ограничивать количество устройств, являющихся источниками логов. - Система должна поддерживать временное увеличение	Обязательно

№	Требование	Соответствие
	нагрузки на 30% без необходимости расширения аппаратных или лицензионных ресурсов. 🕐 Поддержка производителя должна предоставляться сертифицированными инженерами. 🕐 Поддержка должна оказываться в режиме минимум 8/5, без ограничения количества обращений. 🕐 Поддержка должна быть доступна как удаленно, так и на территории заказчика. 🕐 Техническая документация и база знаний по системе должны быть размещены в открытом доступе на официальном сайте производителя. 🕐 Производственная лицензия должна сопровождаться тестовой лицензией, позволяющей обработку минимум 2500 EPS. 🕐 Тестовая лицензия должна поддерживаться на тех же условиях, что и производственная.	
1.82.	Безопасность коммуникаций: - Коммуникация между ключевыми компонентами Модуля (агрегация, ретенция, визуализация данных) должна осуществляться в зашифрованном виде с использованием протокола TLS версии не ниже 1.3. - Шифрование соединения между веб-браузером пользователя и Модулем должно осуществляться с использованием TLS версии не ниже 1.3. - Доступ к модулю -Программный модуль должен иметь графический интерфейс управления, доступный через веб-браузер. Поддерживаемые браузеры: Mozilla Firefox Google Chrome Internet Explorer - Доступ к Модулю должен быть защищен паролем или сертификатом. - Механизм аутентификации пользователей должен быть интегрирован с: 🕐 Microsoft Active Directory (AD) 🕐 LDAP (Lightweight Directory Access Protocol) 🕐 RADIUS (Remote Authentication Dial-In User Service) - Пароли типа Windows AD bind должны храниться в зашифрованном виде. - Программный модуль должен поддерживать механизм единого входа (Single Sign-On, SSO). - Программный модуль должен поддерживать возможность управления временем автоматического завершения сессий пользователей.	Обязательно

№	Требование	Соответствие
1.83.	Управление пользователями и ролями: - Система должна обеспечивать интерфейс управления пользователями и их ролями. - Система должна поддерживать гибкое управление правами доступа к объектам, созданным в системе (поисковые запросы, визуализации, дашборды). - Для каждой роли должен быть предусмотрен механизм разграничения прав по уровням: - Read Only (только просмотр) - Full Access (полный доступ) - Объекты, к которым пользователь не имеет доступа, не должны отображаться в интерфейсе.	Обязательно
1.84.	Программный модуль должен поддерживать автоматический импорт индикаторов компрометации (IoC, Indicator of Compromise) и автоматический поиск соответствующих событий среди накопленных логов за определенный временной период. Программный модуль должен обеспечивать нативную интеграцию с базой данных MISP, включая работу с: - IP-адресами - Хешами зараженных файлов - Доменами - URL-адресами Программный модуль должен поставляться с репозиторием IoC, поддерживаемым и обновляемым производителем. Программный модуль должен обладать нативной интеграцией с фреймворком MITRE ATT&CK.	Обязательно
1.85.	Корреляционные правила, оповещения и обработка инцидентов: - Программный модуль должен содержать базу из минимум 700 предустановленных корреляционных правил. - Программный модуль должен поддерживать мониторинг целостности файлов и системных реестров на отслеживаемых хостах, включая: - Отслеживание изменений содержимого файлов и каталогов - Изменения прав доступа к файлам - Изменения атрибутов файлов - Контроль изменений хеш-сумм MD5 и SHA1	Обязательно
1.86.	Программный модуль должен поддерживать мониторинг конфигурации операционных систем и приложений для обеспечения соответствия стандартам информационной безопасности, таким как: - CIS Benchmark - Hardening-практики	Обязательно

№	Требование	Соответствие
1.87.	Программный модуль должен обеспечивать преднастроенные визуализации и политики соответствия стандартам: - PCI-DSS (Стандарт безопасности данных индустрии платежных карт) - NIST (Национальный институт стандартов и технологий США) - ISO 27001 (Международный стандарт управления информационной безопасностью Программный модуль должен обладать возможностью сканирования окружения для детектирования rootkit'ов и выявления скрытых процессов, файлов и портов. Программный модуль должен обеспечивать сканирование уязвимостей операционных систем Linux и Windows, а также установленных в среде приложений. Программный модуль должен поддерживать непрерывное отслеживание соответствия политикам OpenSCAP.	Обязательно
1.88.	Отчетность и архивирование данных: - Программный модуль должен включать встроенный механизм архивирования данных в виде плоских файлов, с возможностью управления архивами через пользовательскую консоль. - Программный модуль должен поддерживать автоматическую и ручную передачу данных в архив, согласно заданным критериям. - Программный модуль должен обеспечивать возможность восстановления архивированных данных в Программный модуль для последующего онлайн-анализа. - Программный модуль должен поддерживать поиск в сжатых архивах без предварительного разархивирования. - Программный модуль должен обеспечивать создание отчетов по любым данным, хранящимся в Модуле. - Отчеты должны генерироваться вручную или автоматически по заданному расписанию. - Программный модуль должен поддерживать генерацию отчетов в форматы PDF, DOCX и JPEG, с возможностью добавления логотипа заказчика и пользовательских комментариев.	Обязательно

№	Требование	Соответствие
1.89.	Внедрение Модуля. Объем ожидаемых работ по внедрению: - Разработка графика внедрения Модуля. - Проведение предвнедренного анализа и подготовка технического проекта внедрения. - Установка и настройка Модуля. - Подключение источников данных. - Настройка корреляционных правил, отчетов и дашбордов для подключенных источников на основе предустановленных компонентов, поставляемых вместе с Модулем. - Если Программный модуль не содержит предустановленных парсеров, визуализаций, дашбордов и корреляционных правил, поставщик обязан разработать их в ходе внедрения. - На этапе предвнедренного анализа поставщик должен предоставить заказчику на согласование перечень предложенных корреляционных правил, визуализаций и дашбордов в соответствии с подключаемыми источниками данных. - Разработка и проведение тестовых сценариев, проверяющих производительность и корректность функционирования внедренного Модуля в среде заказчика. - Тестовые сценарии должны быть представлены заказчику для согласования. - В состав предложения участника конкурса должны быть включены все вышеперечисленные работы по внедрению, количество человеко-дней не менее 10.	Обязательно
1.90.	Обучение персонала: - Поставщик обязан провести обучение по использованию и администрированию Модуля для (количество) сотрудников заказчика. - Продолжительность обучения — 5 рабочих дней (не менее 40 часов). - Группа обучающихся — не более 5 человек. - Каждый участник обучения должен получить учебные материалы. - Инструкторы, проводящие обучение, должны иметь сертификаты от производителя Модуля, подтверждающие их квалификацию в области администрирования и эксплуатации решения.	Обязательно
1.91.	Сопровождение и техническая поддержка: - Поддержка производителя должна предоставляться сертифицированными инженерами. - Минимальный режим работы технической поддержки – 8/5. - Количество обращений в поддержку не должно быть ограничено, а услуги должны предоставляться как удаленно, так и на территории заказчика. - Услуги по сопровождению Модуля должны соответствовать сертификации ISO 27001:2017.	Обязательно

№	Требование	Соответствие
	Техническая документация и база знаний должны быть размещены в открытом доступе на официальном сайте производителя.	
1.92.	Интеграция с Модулем наблюдения и контроля состояния и производительности цифровых активов банка и с Модулем координации инцидентов ИТ и ИБ: Производитель Модулей должен обеспечить возможность расширения решения с помощью функционального Модуля наблюдения и контроля состояния и производительности цифровых активов банка и Модуля координации инцидентов ИТ и ИБ.	Обязательно

6. Требования к программно-аппаратному комплексу сбора, мониторинга и анализа данных сетевого трафика

№	Требование	Соответствие
2.1.	Иметь форм-фактор для установки в стандартную серверную стойку и иметь высоту	Не более 2RU
2.2.	Иметь установленных процессоров серии не ниже Gold, каждый из которых должен иметь не менее 24 (двадцати четырёх) ядер, работающих на частоте не ниже 3.0 ГГц, поддерживать работу памяти с частотой не менее 2933 МГц, иметь кэш-память объёмом не менее 35 Мбайт. Максимальная рассеиваемая мощность процессора должна быть не более 210 Ватт. Должна быть реализована возможность работы с 64х разрядными приложениями на аппаратном уровне.	Не менее 2
2.3.	Наличие слотов DDR для установки модулей памяти	Не менее 24
2.4.	Должно быть установлено модулей памяти RDIMM объёмом не менее 32ГБ каждый, поддерживающих работу на частоте не менее 3200 МГц	Не менее 16
2.5.	Поддерживать установку жёстких дисков форм-фактора не более 2.5’	Не менее 8
2.6.	Иметь установленных сетевых адаптеров с не менее чем с 2 (двумя) портами 10GBase-T	Не менее 2
2.7.	Иметь на каждом сервере установленных драйвов (устройств) SAS SSD объёмом не менее 1.92 ТБ каждый	Не менее 8
2.8.	Иметь блоков питания мощностью не менее 1600 Вт каждый, с возможностью горячей замены; поддержка резервирования питания; кабели питания C13-C14 должны входить в комплект поставки	Не менее 2
2.9.	Дополнительно в комплект поставки должны входить кабели питания типа Euro с длиной	Не менее 3 м
2.10.	Сервер должен быть укомплектован полным комплектом отказоустойчивых резервированных вентиляторов охлаждения	Обязательно
2.11.	Должен быть совместим как минимум со следующими операционными системами и гипервизорами:	Vmware версии не ниже 7
2.12.	Сервер должен быть укомплектован отдельным независимым портом управления 100/1000 Мбит Ethetnet	Обязательно

2.13.	Сервер должен быть укомплектован монтажными рельсами для установки сервера в стандартную телекоммуникационную стойку 19’’	Обязательно
2.14.	Сервер должен быть укомплектован TPM модулем безопасности	Обязательно
2.15.	Должен иметь встроенные аппаратно-программные средства в комплекте с необходимыми для мониторинга и управления лицензиями для удалённого управления и мониторинга (включая выделенный порт управления)	Обязательно
2.16.	Гарантийный срок на оборудования должен быть не менее 3 лет	Обязательно
2.17.	Программный модуль должен предоставляться в виде виртуального программного обеспечения или программного обеспечения на Linux для установки на программно-аппаратный комплекс и функционировать в режиме постоянной лицензии с поддержкой сроком на 3 года.	Обязательно
2.18.	Программный модуль должен функционировать на базе операционной системы Linux.	Обязательно
2.19.	Программный модуль должен обеспечивать централизованный мониторинг сетевого трафика для выявления аномальной активности.	Обязательно
2.20.	Программный модуль должен позволять получать копию сетевого трафика для анализа.	Обязательно
2.21.	Программный модуль должен обеспечивать сбор и анализ данных NetFlow, включая IPFIX, sFlow, J-Flow, NetFlow v9.	Обязательно
2.22.	Производительность обработки NetFlow должна быть не менее 95 000 Flow в секунду.	Обязательно
2.23.	Должна быть поддержка сохранения сетевых пакетов в формате PCAP.	Обязательно
2.24.	Программный модуль должен обеспечивать анализ сетевого трафика с **возможностью** перехвата и инспекции пакетов в режиме реального времени**.**	Обязательно
2.25.	Программный модуль должен поддерживать анализ следующих протоколов: HTTP, DNS, FTP, SSH.	Обязательно
2.26.	Программный модуль должен обеспечивать глубокий анализ сетевого трафика (L2-L7).	Обязательно
2.27.	Лицензия на Программный модуль не должна ограничивать количество источников данных, из которых поступает трафик или NetFlow.	Обязательно
2.28.	Модуль должен поддерживать корреляцию сетевых данных с логами из Программного модуля сбора и аналитики событий	Обязательно
2.29.	Должна быть реализована интеграция с базами репутации IP-адресов (Bad IP Reputation).	Обязательно
2.30.	Программный модуль должен поддерживать выявление аномалий на основе поведенческого анализа.	Обязательно

2.31.	Программный модуль должен обеспечивать идентификацию zero-day атак и несанкционированного трафика.	Обязательно
2.32.	Модуль должен поддерживать визуализацию сетевых соединений между IP-адресами.	Обязательно
2.33.	В программном модуле должна быть поддержка геолокации событий на основе IP-адресов.	Обязательно
2.34.	Программный модуль должен обеспечивать автоматическую генерацию отчетов по выявленным аномалиям в сети или должна быть бесшовная возможность интегрироваться с системой отчетности Программного модуля сбора и аналитики событий, передавая туда всю необходимую информацию для построения отчетов и дашбордов.	Обязательно
2.35.	Должна быть возможность экспорта данных в CSV, HTML, PDF.	Обязательно
2.36.	Программный модуль должен поддерживать дашборды для анализа сетевого трафика.	Обязательно
2.37.	Программный модуль должен обеспечивать графическое представление трафика с разбивкой по протоколам, IP-адресам и регионам.	Обязательно
2.38.	Внедрение Модуля. Объем ожидаемых работ по внедрению: - Разработку графика внедрения. - Проведение предвнедренного анализа. - Установка и настройку модуля. - Интеграция с программным модулем сбора и аналитики событий - Настройка визуализаций и отчетности. - Подключение источников трафика - Тестирование производительности и корректности функционирования. - Проведение тестов обнаружения угроз. Разработка и проведение тестовых сценариев, проверяющих производительность и корректность функционирования внедренного Модуля в среде заказчика. - Тестовые сценарии должны быть представлены заказчику для согласования. - В состав предложения участника конкурса должны быть включены все вышеперечисленные работы по внедрению, количество человеко-дней не менее 10.	Обязательно

2.39.	Обучение персонала: 🕐 Поставщик обязан провести обучение по использованию и администрированию Модуля для (количество) сотрудников заказчика. 🕐 Продолжительность обучения — 5 рабочих дней (не менее 40 часов). 🕐 Группа обучающихся — не более 5 человек. 🕐 Каждый участник обучения должен получить учебные материалы. 🕐 Инструкторы, проводящие обучение, должны иметь сертификаты от производителя Модуля, подтверждающие их квалификацию в области администрирования и эксплуатации решения.	Обязательно
2.40.	Сопровождение и техническая поддержка: 🕐 Поддержка производителя должна предоставляться сертифицированными инженерами. 🕐 Минимальный режим работы технической поддержки – 8/5. 🕐 Количество обращений в поддержку не должно быть ограничено, а услуги должны предоставляться как удаленно, так и на территории заказчика. 🕐 Услуги по сопровождению Модуля должны соответствовать сертификации ISO 27001:2017. 🕐 Техническая документация и база знаний должны быть размещены в открытом доступе на официальном сайте производителя.	Обязательно
2.41.	Программный модуль должен быть интегрирован с Программным модулем сбора и аналитики событий для передачи данных по аномальному трафику. Инциденты, зафиксированные в модуле, должны автоматически передаваться в Программный модуль аналитики событий для дальнейшего расследования. Программный модуль должен обеспечивать возможность интеграции с Модулем наблюдения и контроля состояния и производительности цифровых активов банка и Модулем координации инцидентов ИТ и ИБ.	Обязательно

7. Требования к программно-аппаратному комплексу наблюдения и контроля состояния и производительности цифровых активов банка

№	Требование	Соответствие
3.1.	Иметь форм-фактор для установки в стандартную серверную стойку и иметь высоту	Не более 2RU
3.2.	Иметь установленных процессоров серии не ниже Gold, каждый из которых должен иметь не менее 24 (двадцати четырёх) ядер, работающих на частоте не ниже 3.0 ГГц, поддерживать работу памяти с частотой не менее 2933 МГц, иметь кэш-память объёмом не менее 35 Мбайт. Максимальная рассеиваемая мощность процессора должна быть не более 210 Ватт. Должна быть реализована возможность работы с 64х разрядными приложениями на	Не менее 2

	аппаратном уровне.	
3.3.	Наличие слотов DDR для установки модулей памяти	Не менее 24
3.4.	Должно быть установлено модулей памяти RDIMM объёмом не менее 32ГБ каждый, поддерживающих работу на частоте не менее 3200 МГц	Не менее 16
3.5.	Поддерживать установку жёстких дисков форм-фактора не более 2.5’	Не менее 8
3.6.	Иметь установленных сетевых адаптеров с не менее чем с 2 (двумя) портами 10GBase-T	Не менее 2
3.7.	Иметь на каждом сервере установленных драйвов (устройств) SAS SSD объёмом не менее 1.92 ТБ каждый	Не менее 8
3.8.	Иметь блоков питания мощностью не менее 1600 Вт каждый, с возможностью горячей замены; поддержка резервирования питания; кабели питания C13-C14 должны входить в комплект поставки	Не менее 2
3.9.	Дополнительно в комплект поставки должны входить кабели питания типа Euro с длиной	Не менее 3 м
3.10.	Сервер должен быть укомплектован полным комплектом отказоустойчивых резервированных вентиляторов охлаждения	Обязательно
3.11.	Должен быть совместим как минимум со следующими операционными системами и гипервизорами:	Vmware версии не ниже 7
3.12.	Сервер должен быть укомплектован отдельным независимым портом управления 100/1000 Мбит Ethetnet	Обязательно
3.13.	Сервер должен быть укомплектован монтажными рельсами для установки сервера в стандартную телекоммуникационную стойку 19’’	Обязательно
3.14.	Сервер должен быть укомплектован TPM модулем безопасности	Обязательно
3.15.	Должен иметь встроенные аппаратно-программные средства в комплекте с необходимыми для мониторинга и управления лицензиями для удалённого управления и мониторинга (включая выделенный порт управления)	Обязательно
3.16.	Гарантийный срок на оборудования должен быть не менее 3 лет	Обязательно
3.17.	Программный модуль должен предоставляться в виде виртуального программного обеспечения или программного обеспечения на Linux для установки на программно-аппаратный комплекс и функционировать в режиме постоянной лицензии с поддержкой сроком на 3 года. Лицензия должна позволять работать одновременно с 500 IP-адресами. Дополнительно: • Программный модуль должен обеспечивать доступность в коммерческой версии, готовой к установке и настройке в инфраструктуре банка. • Программный модуль должен официально распространяться на территории Республики Узбекистан. • Лицензирование должно осуществляться на основании количества уникальных мониторируемых IP-адресов.	Обязательно

	• Лицензия не должна ограничивать количество метрик, отслеживаемых в рамках одного IP-адреса. • Программный модуль должен поставляться в последней актуальной версии. • Программный модуль должен сопровождаться технической поддержкой от производителя не менее 3 лет (обновления до актуальной версии, техническая поддержка). • Программный модуль должен иметь официальную поддержку от производителя. Решения, у которых поддержка основана исключительно на сообществе пользователей, не принимаются к рассмотрению. • В комплект поставки должны входить документация, инструкции по настройке и эксплуатации.	
3.18.	Мониторинг серверов и сетевого оборудования: Программный модуль должен обеспечивать: • мониторинг серверов и рабочих станций, входящих в ИТ-инфраструктуру банка; • поддержку операционных систем Windows, Linux, Unix, IBM AIX; • мониторинг сетевого оборудования (маршрутизаторы, коммутаторы, межсетевые экраны); • отслеживание физических ресурсов серверов и рабочих станций (ЦПУ, оперативная память, дисковое пространство).	Обязательно
3.19.	Мониторинг банковских приложений и сервисов: Программный модуль должен обеспечивать: • контроль доступности и производительности приложений, веб-приложений и баз данных; • поддержку мониторинга облачных сервисов (AWS, Azure, Google Cloud); • мониторинг критичных сервисов банка (HTTP, HTTPS, FTP, SMTP, DNS и др.).	Обязательно
3.20.	Мониторинг пользователей и веб-приложений банка: Программный модуль должен обеспечивать: • автоматизированное тестирование пользовательских сценариев в банковских веб-приложениях; • мониторинг производительности банковских приложений с точки зрения конечного пользователя; • контроль параметров времени загрузки страниц и последовательности пользовательских действий.	Обязательно
3.21.	Оповещения и уведомления: Программный модуль должен предоставлять возможность: • настройки пороговых значений и автоматических уведомлений (email, SMS, PUSH-уведомления); • гибкой настройки оповещений в зависимости от критичности	Обязательно

	инцидента; - интеграции с банковскими системами управления инцидентами (ITSM); - эскалации уведомлений.	
3.22.	Отчетность и анализ данных: Программный модуль должен обеспечивать: - генерацию отчетов по доступности, производительности и использованию ресурсов ИТ-инфраструктуры банка; - возможность визуализации данных в виде графиков и дашбордов для удобного анализа ключевых метрик; - экспорт отчетов в распространенные форматы (PDF, CSV); - формирование и редактирование отчетов через веб-интерфейс без необходимости установки дополнительного ПО. Инструмент отчетности в Модуле должен обеспечивать автоматическую генерацию отчетов по заранее заданному расписанию, включая: - отчеты по доступности (по хостам или сервисам); - отчеты по SLA (по хостам или сервисам); - отчеты по инцидентам и отказам; - отчеты по производительности сети. Дополнительно, Программный модуль должен поддерживать: - автоматическое сохранение отчетов в формате PDF; - периодическую отправку отчетов по электронной почте; - уведомления о событиях по электронной почте; - сохранение заданных параметров отчетов для их повторного использования.	Обязательно

3.23.	Автоматизация и оркестрация: Программный модуль должен поддерживать: - автоматическую конфигурацию новых устройств, добавляемых в ИТ-инфраструктуру банка; - автоматическое выполнение скриптов в ответ на определенные события, возникающие в процессе мониторинга; - интеграции с инструментами управления конфигурациями (Ansible, Puppet, Chef); - возможность планирования и выполнения задач с учетом расписания; - автоматическое добавление метрик (датчиков измерений) для новых аппаратных компонентов; - автоматическое обновление информации о сетевых интерфейсах при изменении их имен и описаний.	Обязательно
3.24.	Безопасность и аудит: Программный модуль должен обеспечивать: - зашифрованный обмен данными между своими компонентами; - мониторинг и аудит событий, связанных с безопасностью; - создание резервных копий конфигурации системы; - управление пользователями и возможность создания групп пользователей с различными уровнями доступа; - хранение исторических статистических данных для анализа. Механизм назначения прав пользователей должен включать: - доступ к данным по хостам и сервисам; - возможность изменения конфигурации объектов; - настройку и получение уведомлений. - Программный модуль должен вести аудит активности пользователей, фиксируя все изменения, внесенные в настройки, а также действия, связанные с управлением и мониторингом объектов.	Обязательно

3.25.	Интеграции и API: Программный модуль должен обладать: - открытым API для интеграции с другими информационными системами банка; - интеграциями с популярными инструментами управления ИТ-активами и процессами (ServiceNow, Jira); - нативной интеграцией с централизованными системами сбора логов и анализа событий (Elasticsearch, Opensearch); - нативной интеграцией с SOAR-системами для автоматизации реагирования на инциденты; - поддержкой webhooks для передачи данных в реальном времени.	Обязательно
3.26.	Пользовательский интерфейс: Программный модуль должен предоставлять: - графический интерфейс для визуализации сетевой структуры; - графическое представление параметров выбранных устройств; - дружественный и интуитивно понятный интерфейс, доступный через веб-браузер. Программный модуль должен поддерживать: - персонализацию основного экрана приложения для пользователей; - возможность создания нескольких дашбордов для отображения различных аспектов мониторинга; - поддержку персональных и общих дашбордов, которые могут быть разделены с другими пользователями; - создание iFrame-дашбордов, отображающих данные из внешних приложений; - поддержку добавления пользовательских виджетов в дашборды. Дополнительно, Программный модуль должен обеспечивать: - возможность создания и сохранения фильтров для мониторируемых устройств и их параметров; - возможность использования фильтров при создании дашбордов; - поддержку режима "день/ночь" для комфортной работы в разных условиях освещения.	Обязательно

3.27.	Мониторинг ключевых параметров банковской инфраструктуры: Программный модуль должен обеспечивать мониторинг: - базовых аппаратных параметров без необходимости установки дополнительных агентов; - параметров работы операционной системы и сервисов с использованием специализированных агентов; - критически важных элементов инфраструктуры банка, включая: - приложения; - сетевые сервисы; - сетевые протоколы; - системные индикаторы; - элементы сетевой инфраструктуры; - порты. Мониторинг почтовых систем банка должен включать: - проверку работоспособности SMTP, POP3 и IMAP-серверов; - контроль количества сообщений в очередях почтового сервера Postfix. Мониторинг DNS-сервисов банка должен включать: - проверку работоспособности DNS-сервера; - контроль корректности разрешения доменов в IP-адреса. Мониторинг веб-серверов банка должен включать: - проверку работоспособности веб-сервера; - контроль наличия ожидаемого контента на веб-странице; - контроль времени отклика веб-сервера.	Обязательно
3.28.	Архитектура и производительность: Программный модуль должен поддерживать: - клиент-серверную модель; - развертывание в локальной инфраструктуре (on-premises) или в облаке; - горизонтальное и вертикальное масштабирование; - архитектуру высокой доступности (HA); - хранение данных в нереляционной базе данных; - настройку резервного копирования и восстановления данных через графический интерфейс.	Обязательно

3.29.	Техническая поддержка: Программный модуль должен сопровождаться: • технической поддержкой уровня не ниже 8/5 (8 часов в день, 5 дней в неделю); • доступом к базе знаний и технической документации; • возможностью приобретения расширенной поддержки от производителя, включая: • текущее администрирование системы; • регулярные проверки работоспособности (health checks); • подключение новых точек мониторинга; • создание новых визуализаций; • изменения в архитектуре системы.	Обязательно
3.30.	Обучение персонала: • Поставщик обязан провести обучение по использованию и администрированию Модуля для (количество) сотрудников заказчика. • Продолжительность обучения — 5 рабочих дней (не менее 24 часов). • Группа обучающихся — не более 5 человек. • Каждый участник обучения должен получить учебные материалы. Инструкторы, проводящие обучение, должны иметь сертификаты от производителя Модуля, подтверждающие их квалификацию в области администрирования и эксплуатации решения.	Обязательно
3.31.	Требования к внедрению Модуля: Внедрение Модуля в ИТ-инфраструктуру банка должно включать: • полный цикл работ, включая установку, настройку, интеграцию с существующими системами и тестирование работоспособности; • предоставление инженеров для выполнения работ по внедрению (не менее 20 рабочих дней); • работы в соответствии с согласованным техническим планом; • подтверждение квалификации специалистов сертификатами не менее чем двух инженеров; • предоставление отчетов о проделанной работе и документации по настройкам после завершения внедрения.	Обязательно

8. Требования к программно-аппаратному комплексу координации инцидентов ИТ и ИБ

№	Требование	Соответствие
4.1.	Иметь форм-фактор для установки в стандартную серверную стойку и иметь высоту	Не более 2RU
4.2.	Иметь установленных процессоров серии не ниже Gold, каждый из которых должен иметь не менее 24 (двадцати четырёх) ядер, работающих на частоте не ниже 3.0 ГГц, поддерживать работу	Не менее 2

	памяти с частотой не менее 2933 МГц, иметь кэш-память объёмом не менее 35 Мбайт. Максимальная рассеиваемая мощность процессора должна быть не более 210 Ватт. Должна быть реализована возможность работы с 64х разрядными приложениями на аппаратном уровне.	
4.3.	Наличие слотов DDR для установки модулей памяти	Не менее 24
4.4.	Должно быть установлено модулей памяти RDIMM объёмом не менее 32ГБ каждый, поддерживающих работу на частоте не менее 3200 МГц	Не менее 16
4.5.	Поддерживать установку жёстких дисков форм-фактора не более 2.5’	Не менее 8
4.6.	Иметь установленных сетевых адаптеров с не менее чем с 2 (двумя) портами 10GBase-T	Не менее 2
4.7.	Иметь на каждом сервере установленных драйвов (устройств) SAS SSD объёмом не менее 1.92 ТБ каждый	Не менее 8
4.8.	Иметь блоков питания мощностью не менее 1600 Вт каждый, с возможностью горячей замены; поддержка резервирования питания; кабели питания C13-C14 должны входить в комплект поставки	Не менее 2
4.9.	Дополнительно в комплект поставки должны входить кабели питания типа Euro с длиной	Не менее 3 м
4.10.	Сервер должен быть укомплектован полным комплектом отказоустойчивых резервированных вентиляторов охлаждения	Обязательно
4.11.	Должен быть совместим как минимум со следующими операционными системами и гипервизорами:	Vmware версии не ниже 7
4.12.	Сервер должен быть укомплектован отдельным независимым портом управления 100/1000 Мбит Ethetnet	Обязательно
4.13.	Сервер должен быть укомплектован монтажными рельсами для установки сервера в стандартную телекоммуникационную стойку 19’’	Обязательно
4.14.	Сервер должен быть укомплектован TPM модулем безопасности	Обязательно
4.15.	Должен иметь встроенные аппаратно-программные средства в комплекте с необходимыми для мониторинга и управления лицензиями для удалённого управления и мониторинга (включая выделенный порт управления)	Обязательно
4.16.	Гарантийный срок на оборудования должен быть не менее 3 лет	Обязательно
4.17.	Программный модуль должен поддерживать работу команд реагирования на инциденты (SOC, CERT, CSIRT, IRT и др.), включая: Мониторинг кибербезопасности; Реагирование на инциденты; Управление уязвимостями; Стандартизацию и автоматизацию работы аналитиков ИБ.	Обязательно
4.18.	Программный модуль должен нативно интегрироваться с SIEM-системой Банка. Производитель Модуля должен официально поддерживать интеграцию с используемой SIEM-системой.	Обязательно

4.19.	Программный модуль должен автоматически создавать инциденты на основании уведомлений SIEM, сообщений пользователей на выделенный email, тикетов в системе helpdesk Банка (минимально RTIR или Jira). Должна быть поддержка автоматического закрытия инцидента в helpdesk после его обработки (минимально RTIR или Jira).	Обязательно
4.20.	Программный модуль должен поддерживать возможность ручного создания инцидентов.	Обязательно
4.21.	Программный модуль должен обеспечивать автоматическую и ручную классификацию инцидентов по уровню критичности.	Обязательно
4.22.	Программный модуль должен позволять создание пользовательских классификаций инцидентов и их критичности. В рамках внедрения Подрядчик совместно с Заказчиком должен согласовать и настроить классификацию.	Обязательно
4.23.	Программный модуль должен отслеживать время обработки инцидентов, включая метрики Time-to-Detect (TTD) и Time-to-Mitigate (TTM).	Обязательно
4.24.	Программный модуль должен поддерживать возможность объединения инцидентов, включая автоматическое интеллектуальное объединение.	Обязательно
4.25.	Программный модуль должен автоматически назначать предопределенные задачи для разных типов инцидентов.	Обязательно
4.26.	Программный модуль должен поддерживать визуальное создание и редактирование сценариев реагирования на инциденты с возможностью использования логических и математических операторов.	Обязательно
4.27.	Программный модуль должен поддерживать автоматическое и ручное назначение инцидентов конкретным сотрудникам.	Обязательно
4.28.	Программный модуль должен поддерживать автоматизированную и ручную проверку атрибутов инцидентов во внутренних и внешних базах данных.	Обязательно
4.29.	Программный модуль должен поддерживать проектирование и реализацию автоматизированных ответных действий на инциденты.	Обязательно
4.30.	Программный модуль должен позволять редактирование исходного кода автоматизированных сценариев реагирования. Должен использоваться современный скриптовый язык (например, Python 3).	Обязательно
4.31.	Программный модуль должен поддерживать создание сводных отчетов по зарегистрированным и обработанным инцидентам.	Обязательно
4.32.	Программный модуль должен интегрироваться как минимум с: Microsoft Exchange (получение и отправка email); CheckPoint Duo_Security Eset FortiMail Gmail MS Defender Endpoints	Обязательно

	MS Defender Office365 PaloAlto Cortex XDR PaloAlto NGFW IBM Qradar SentinelOne Shuffle Cisco Umbrella Wazuh Slack (отправка сообщений). Telegram (отправка сообщений).	
4.33.	Программный модуль должен иметь в базовой инсталляции подключенные и готовые к использованию такие базы индикатором компрометации, как (минимум): AbuseIPDB Abuse_Finder AnyRun Autofocus BackscatterIO BitcoinAbuse C1fApp CERTatPassiveDNS CIRCLHashlookup CIRCLPassiveDNS CIRCLPassiveSSL CISMCAP Censys CheckPhish ClamAV Crowdsec Crtsh CuckooSandbox CyberChef CyberCrime-Tracker Cyberprotect Cylance Cylance hashlookup DShield Diario DomainMailSPFDMARC DomainTools DomainToolsIris EchoTrail Elasticsearch EmailRep EmergingThreats EmlParser EnrichmentEngine	Обязательно

- FalconSandbox
- FileInfo
- FireEyeiSight
- FireHOLBlocklists
- ForcepointWebsensePing
- Fortiguard
- GRR
- GreyNoise
- Hippocampe
- Hunterio
- HybridAnalysis
- IBM XForce
- IP-API
- IPVoid
- IPinfo
- IVRE
- Inoitsu
- KasperskyTIP
- LastInfoSec
- LdapQuery
- MISP
- MISPWarningLists
- Malpedia
- Maltiverse
- MalwareBazaar
- MalwareClustering
- Malwares
- MaxMind
- MetaDefender
- MnemonicPDNS
- MsgParser
- NERD
- NSRL
- Nessus
- OTXQuery
- Onyphe
- OpenCTI
- PaloAltoWildFire
- PassiveTotal
- Patrowl
- PayloadSecurity
- PhishTank
- PhishingInitiative
- ProofPoint
- Pulsedive
- RecordedFuture
- RiskIQ
- Robtex

	SEKOIAIntelligenceCenter SecurityTrails SentinelOne Shodan SinkDB SoltraEdge SophosIntelix SpamAssassin SpamhausDBL StamusNetworks StaxxSearch StopForumSpam TalosReputation TeamCymruMHR ThreatGrid ThreatMiner ThreatResponse Threatcrowd Thunderstorm TorBlutmagie TorProject Triage Triage Sandbox analyzer URLhaus Umbrella UnshortenLink Urlscan.io VMRay Valhalla Verifalia VirusTotal Virusshare Vulners WOT Yara Yeti Zscaler	
4.34.	Программный модуль должен поддерживать интеграцию с другими системами класса Threat Intelligence / Threat Hunting / Threat Sharing через API.	Обязательно
4.35.	Программный модуль должен обеспечивать создание аналитических дашбордов по данным SOAR (например, статистика инцидентов) с возможностью настройки главного экрана для SOC.	Обязательно
4.36.	Программный модуль должен поддерживать двустороннюю связь с пользователями (например, для сбора дополнительной информации по инциденту) через интерактивные формы.	Обязательно
4.37.	Программный модуль должен обеспечивать более 250 готовых интеграций для двустороннего взаимодействия с внешними	Обязательно

	системами.	
4.38.	Программный модуль должен автоматизировать анализ данных, включая: Автоматическую проверку файлов в sandbox; Уведомление пользователей об угрозах (email, мессенджеры); Автоматическое ограничение сетевого доступа.	Обязательно
4.39.	Программный модуль должен содержать не менее 5 предустановленных типов инцидентов с возможностью их редактирования и копирования.	Обязательно
4.40.	Программный модуль должен поддерживать использование внешних библиотек и программ в скриптах (например, запуск сценариев в контейнерах с дополнительным ПО).	Обязательно
4.41.	Программный модуль должен предоставлять доступ к коду интеграций с возможностью их копирования и модификации.	Обязательно
4.42.	Программный модуль должен поддерживать графическое создание сценариев реагирования (playbook) без необходимости программирования.	Обязательно
4.43.	Программный модуль должен поддерживать вложенные сценарии (главный сценарий может вызывать подчиненные).	Обязательно
4.44.	Программный модуль должен позволять создание сценариев, содержащих: a. задачи, поставленные и настроенные вручную; b. автоматизированные задачи; c. автоматические условные задачи; d. задачи, поставленные и настроенные вручную, с учетом условий; e. сбор данных с использованием форм; f. фильтрацию данных; g. под-сценарии.	Обязательно
4.45.	Программный модуль должен позволять автоматическое документирование выполнения сценариев.	Обязательно
4.46.	Программный модуль должен обеспечивать визуализацию выполнения сценариев (логика работы, пропущенные задачи, решения операторов и т. д.).	Обязательно
4.47.	Программный модуль должен поддерживать управление сценариями через email и мессенджеры (Teams, Telegram, Slack, Mattermost и др.).	Обязательно
4.48.	Программный модуль должен поддерживать отладку сценариев в пошаговом режиме.	Обязательно
4.49.	Программный модуль должен позволять повторный запуск сценариев на конкретных инцидентах.	Обязательно
4.50.	Программный модуль должен поддерживать срочный запуск автоматизированных задач без изменения сценариев.	Обязательно
4.51.	Программный модуль должен позволять мониторинг выполнения сценариев и оповещение ответственных лиц о сбоях.	Обязательно
4.52.	Программный модуль должен поддерживать: 🕐 Делегирование задач между сотрудниками SOC; 🕐 Передачу параметров между задачами; 🕐 Анализ результатов сценариев.	Обязательно

4.53.	Программный модуль должен позволять простое мониторирование состояния выполнения сценариев, связанных с инцидентами. Кроме того, в случае возникновения любых аномалий в процессе выполнения сценария, ответственные за инцидент лица должны быть немедленно уведомлены.	Обязательно
4.54.	Программный модуль должен позволять назначение задач в рамках одного сценария разным членам команды SOC.	Обязательно
4.55.	Программный модуль должен позволять передачу параметров между задачами в рамках одного сценария.	Обязательно
4.56.	Программный модуль должен позволять считывание результатов анализа и их использование в последующих задачах выполняемого сценария.	Обязательно
4.57.	Программный модуль должен позволять просмотр исторических данных о выполненных сценариях и задачах.	Обязательно
4.58.	Программный модуль должен позволять запуск сценариев в заранее определенное время и в соответствии с расписанием.	Обязательно
4.59.	Программный модуль должен позволять проверку того, какие инциденты остались необработанными.	Обязательно
4.60.	Программный модуль должен позволять создание собственных: a. Типов инцидентов b. Полей/меток инцидентов c. Типов индикаторов (Indicator) d. Полей/меток индикаторов (Indicator) e. Отчетов f. Дашбордов	Обязательно
4.61.	Программный модуль должен позволять автоматическое заполнение полей инцидента на основе его типа или атрибутов.	Обязательно
4.62.	Программный модуль должен позволять делегирование задач другим членам команды SOC в рамках оценки данного инцидента.	Обязательно
4.63.	Программный модуль должен позволять взаимодействие между членами команды SOC (например, обсуждение инцидента между сотрудниками).	Обязательно
4.64.	Программный модуль должен позволять сохранение исторических инцидентов с полной информацией о предпринятых мерах по обработке/решению инцидента для обучения и передачи знаний между членами команды SOC. История инцидента должна включать: 🕐 результаты выполнения автоматических и вручную настроенных задач, указанных в playbook; 🕐 комментарии аналитиков, работающих с инцидентом; 🕐 индикаторы компрометации (IoC), такие как IP-адреса, URL, домены и др., автоматически извлеченные и вручную отмеченные во время обработки инцидента; 🕐 элементы анализа, отмеченные аналитиками как доказательства (например, скриншоты подозрительных веб-страниц); 🕐 файлы, добавленные аналитиками в историю обработки инцидента.	Обязательно

4.65.	Программный модуль должен позволять экспорт индикаторов компрометации на серверы MISP.	Обязательно
4.66.	Программный модуль должен позволять импорт событий с серверов MISP.	Обязательно
4.67.	Программный модуль должен позволять экспорт инцидентов в форматах STIX 1/2, CSV, DOCX, PDF.	Обязательно
4.68.	Программный модуль должен позволять создание нескольких экземпляров интеграции одного типа для сторонних решений (например, две интеграции с серверами IMAP или обработку данных threat intelligence из двух разных источников в формате JSON).	Обязательно
4.69.	Программный модуль должен позволять расширение функциональных возможностей путем создания и редактирования сценариев за счет добавления пользовательских скриптов, реализующих: 🕐 нестандартную логику условных операций, 🕐 фильтрацию и модификацию данных, 🕐 кастомную визуализацию данных в дашбордах, 🕐 автоматические задачи, выполняемые после завершения обработки инцидента и др.	Обязательно
4.70.	Программный модуль должен позволять простое добавление глобальных наборов учетных данных, что облегчит использование единого технического аккаунта для нескольких интеграций с внешними системами.	Обязательно
4.71.	Программный модуль должен содержать набор предопределенных отчетов, включая: 🕐 отчет о инцидентах: дневной, 7-дневный и 30-дневный; 🕐 отчет о среднем времени решения инцидента.	Обязательно
4.72.	Программный модуль должен позволять создание пользовательских отчетов и дашбордов с использованием предопределенных компонентов визуализации данных (например, круговые диаграммы, столбчатые диаграммы, линейные графики, таблицы и т. д.).	Обязательно
4.73.	Программный модуль должен позволять простое поиск инцидентов на основе их характеристик (например, с использованием специализированного языка запросов) и их схожести с другими инцидентами (related incidents).	Обязательно
4.74.	Программный модуль должен позволять визуализацию взаимосвязей между похожими инцидентами на уровне совпадения идентичных индикаторов компрометации.	Обязательно
4.75.	Программный модуль должен позволять экспорт отчетов в форматах: a. PDF b. DOCX	Обязательно
4.76.	Программный модуль должен поддерживать работу в режиме мультиарендности (multi-tenant), обеспечивая полную изоляцию ресурсов и данных для различных организаций/клиентов.	Обязательно
4.77.	Программный модуль должен обладать репозиторием индикаторов	Обязательно

	компрометации (IoC), который собирает и коррелирует индикаторы угроз во всех инцидентах, оповещениях и полученных потоках данных.	
4.78.	Программный модуль должен поддерживать выполнение сценариев на основе набора индикаторов, определенных пользователем.	Обязательно
4.79.	Программный модуль должен поддерживать обработку структурированных форматов данных, таких как JSON, CSV, STIX 1.X и STIX 2.X, при интеграции с источниками индикаторов компрометации.	Обязательно
4.80.	Программный модуль должен поддерживать как минимум следующие типы индикаторов компрометации (IoC): a. номера платежных карт b. IBAN c. адрес электронной почты d. учетная запись пользователя e. результаты CVE f. доменное имя g. FQDN h. имя хоста i. IP-адреса (IPv4 и IPv6) j. ключ и путь реестра k. URL l. CIDR	Обязательно
4.81.	Программный модуль должен позволять создание собственных определений индикаторов, их полей и скриптов репутации.	Обязательно
4.82.	Программный модуль должен обеспечивать пользователям возможность автоматической верификации индикаторов (так называемый enrichment), выполняя соответствующий сценарий или запуская проверку на основе типа индикатора (indicator).	Обязательно
4.83.	Программный модуль должен иметь нативную интеграцию с MITRE ATT&CK и привязывать к инцидентам соответствующие тактики и техники.	Обязательно
4.84.	Программный модуль должен быть масштабируемым – обеспечивать возможность легкого расширения (возможность увеличения архитектуры за счет дополнительных серверов/устройств без необходимости внесения изменений в программный код). Конструкция Модуля должна обеспечивать гибкое масштабирование.	Обязательно
4.85.	В рамках Модуля должны применяться механизмы, обеспечивающие высокую доступность, в частности кластерные технологии с использованием виртуализации. Архитектура Модуля должна гарантировать отказоустойчивость отдельных элементов, чтобы сбой любого компонента не приводил к недоступности всей системы.	Обязательно
4.86.	В состав решения должны входить механизмы, обеспечивающие высокую производительность всех компонентов, в частности серверов Модуля, веб-интерфейса и баз данных. Обязательно, чтобы решение поддерживало масштабирование	Обязательно

	производительности путем добавления дополнительных серверов приложений/веб-серверов.	
4.87.	Клиентские приложения не могут напрямую взаимодействовать с базой данных.	Обязательно
4.88.	Все компоненты Модуля должны регулярно обновляться. Операционные системы, базы данных и все системные компоненты должны поддерживать установку обновлений и новых версий, предоставляемых их производителем, особенно обновлений безопасности.	Обязательно
4.89.	Все серверные компоненты, приложения и сервисы Модуля должны запускаться как системные службы.	Обязательно
4.90.	Программный модуль должен интегрироваться с Active Directory на платформе Windows Server 2019 и выше для аутентификации пользователей. Должен использоваться механизм входа с логином и паролем Active Directory для администраторов.	Обязательно
4.91.	Доступ к Модулю должен осуществляться через веб-браузер. Все передаваемые данные должны быть зашифрованы с использованием протокола TLS. Программный модуль должен поддерживать сертификаты SSL (предоставленные Заказчиком от внутреннего или коммерческого центра сертификации) для веб-серверов, а передача данных должна осуществляться по протоколу HTTPS.	Обязательно
4.92.	Требования к веб-интерфейсу Модуля: 🕐 Не допускается использование компонентов ActiveX и NPAPI. 🕐 Запрещено использование Flash, Silverlight, Java-апплетов или иных технологий, не поддерживаемых стандартами W3C. 🕐 Визуальный слой интерфейса должен быть реализован в HTML5, XHTML 1.1 или с использованием CSS3. 🕐 Код веб-страниц должен корректно работать в актуальных версиях браузеров Microsoft Edge, Google Chrome (на платформе Windows). 🕐 Подрядчик должен гарантировать совместимость Модуля с актуальными версиями перечисленных браузеров в течение срока технической поддержки. 🕐 Весь сетевой трафик между компонентами Модуля должен быть зашифрован с использованием современных криптографических алгоритмов. Допускается использование: 🕐 TLS 1.2, SSH 2 и их более новых версий; 🕐 TLS 1.3 при взаимодействии с веб-браузером; Не допускается использование SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1.	Обязательно
4.93.	Программный модуль должен поддерживать сертифицированные X.509 сертификаты, предоставленные Заказчиком.	Обязательно
4.94.	Аутентификация администраторов Модуля должна базироваться на ролях пользователей. Решение должно поддерживать иерархическую модель распределения привилегий с возможностью их назначения и отзыва через администратора Модуля или Active Directory.	Обязательно

4.95.	Программный модуль должен поддерживать работу не менее чем 2 одновременных пользователей с разными ролями.	Обязательно
4.96.	Программный модуль должен поддерживать аутентификацию через внешние серверы Active Directory.	Обязательно
4.97.	Для каждого администратора должно быть создано уникальное учетное имя, позволяющее его однозначную идентификацию. Этот идентификатор должен совпадать с учетной записью пользователя в Active Directory.	Обязательно
4.98.	Хранение паролей в Модуле должно осуществляться с применением безопасных криптографических хэш-функций с использованием солей (Hashing with Salt).	Обязательно
4.99.	Программный модуль должен содержать журнал событий (аудит), в котором фиксируются все операции и выполненные пользователями команды. Журнал должен быть доступен для анализа и настройки автоматического мониторинга активности операторов.	Обязательно
4.100.	Заказчик оставляет за собой право контролировать процесс установки Модуля и участвовать в нем. Подрядчик должен предоставить инструкции по установке и настройке всех компонентов.	Обязательно
4.101.	Программный модуль не должен требовать удаленного доступа к продуктивному окружению Заказчика.	Обязательно
4.102.	Подрядчик должен предоставить документированную архитектуру Модуля, включающую: 🕐 Описание всех серверных компонентов. 🕐 Технические параметры серверов. 🕐 Названия и IP-адреса компонентов. 🕐 Схему соединений между компонентами с указанием направлений трафика, портов TCP/UDP и используемых протоколов. 🕐 Вся техническая документация, проектные и эксплуатационные материалы должны быть предоставлены на русском языке или английском языке.	Обязательно
4.103.	Подрядчик обязан предоставить рекомендации по настройке Модуля, включая минимальные необходимые сетевые и системные требования (например, детальные параметры разрешенных сетевых соединений, порты TCP/UDP, требования к доступу к каталогам).	Обязательно
4.104.	Программный модуль должен быть включен в систему резервного копирования, уже действующую у Заказчика. Минимально должна обеспечиваться возможность создания резервных копий конфигурации.	Обязательно
4.105.	Все конфигурации Модуля, включая ОС, базы данных, серверные приложения и другие компоненты, должны проходить процесс hardening в соответствии с CIS Benchmarks и общепризнанными стандартами безопасности.	Обязательно
4.106.	Программный модуль должен быть развернут в инфраструктуре Заказчика (on-premises). Запрещено требование постоянного соединения с внешними серверами лицензирования или передачи	Обязательно

	данных за пределы инфраструктуры Заказчика.	
4.107.	Программный модуль и его компоненты не должны требовать подключения к Интернету для работы. Единственным исключением могут быть обновления сигнатур угроз.	Обязательно
4.108.	Все используемые протоколы и криптографические алгоритмы должны соответствовать современным стандартам безопасности.	Обязательно
4.109.	Внедрение Модуля Объем ожидаемых работ по внедрению: Разработка графика внедрения Модуля. Проведение предвнедренного анализа и подготовка технического проекта внедрения. Установка и настройка Модуля. Подключение источников данных. Настройка корреляционных правил, отчетов и дашбордов для подключенных источников на основе предустановленных компонентов, поставляемых вместе с Модулем. Если Программный модуль не содержит предустановленных парсеров, визуализаций, дашбордов и корреляционных правил, поставщик обязан разработать их в ходе внедрения. На этапе предвнедренного анализа поставщик должен предоставить заказчику на согласование перечень предложенных корреляционных правил, визуализаций и дашбордов в соответствии с подключаемыми источниками данных. Разработка и проведение тестовых сценариев, проверяющих производительность и корректность функционирования внедренного Модуля в среде заказчика. Тестовые сценарии должны быть представлены заказчику для согласования. В состав предложения участника конкурса должны быть включены все вышеперечисленные работы по внедрению, количество человеко-дней не менее 25.	Обязательно
4.110.	Обучение персонала: Поставщик обязан провести обучение по использованию и администрированию Модуля для (количество) сотрудников заказчика. Продолжительность обучения — не менее 2 рабочих дня (не менее 16 часов). Группа обучающихся — не более 5 человек. Каждый участник обучения должен получить учебные материалы. Инструкторы, проводящие обучение, должны иметь сертификаты от производителя Модуля, подтверждающие их квалификацию в области администрирования и эксплуатации решения.	Обязательно
4.111.	Сопровождение и техническая поддержка: Поддержка производителя должна предоставляться сертифицированными инженерами. Программный модуль должен сопровождаться технической поддержкой от производителя не менее 3 лет.	Обязательно

	Минимальный режим работы технической поддержки – 8/5. Количество обращений в поддержку не должно быть ограничено, а услуги должны предоставляться как удаленно, так и на территории заказчика. Услуги по сопровождению Модуля должны соответствовать сертификации ISO 27001:2017. Техническая документация и база знаний должны быть размещены в открытом доступе на официальном сайте производителя.	

Boshqaruv Raisi o'rinbosari: **D.Umarov**

kelishuvchilar: A.Ergashev, V.Krasnov

https://hujjat.sqb.uz/?pin=nJ51cN28&id=878d5d84-3fe1-4ba0-9c6a-fb35185ccca5