**Опросный лист**

**для составления технико-коммерческого предложения**

**на внедрение Системы сбора и анализа событий информационной безопасности «SAVA»**

1. **Общая информация**

| Параметр | Значение (Ответ) |
| --- | --- |
| Общие сведения |
| Общее количество площадок, включая головной офис (ГО), подлежащих мониторингу |  |
| Предполагается ли централизация обработки информации о событиях ИБ? | Да [ ]  | Нет [ ]  |
| Предполагается ли централизованное хранение информации о событиях ИБ?  | Да [ ]  | Нет [ ]  |
| Предполагается ли установка компонентов SAVA на виртуальные платформы? | Да [ ]  | Нет [ ]  |
| Срок хранения нормализованных данных в оперативном доступе (дней) |  |
| Срок хранения исходных (ненормализованных, «сырых») данных в оперативном доступе (дней) |  |
| Выполнение нормативных требований |
| Общие требования (указать основные нормативные акты) |  |
| Отраслевые требования (указать основные нормативные акты) |  |
| Международные требования (указать основные нормативные акты) |  |
| Предполагается ли категоризация информационных системпо требованиям Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»? | Да [ ]  | Нет [ ]  |
| Иные нормативные требования (при наличии, указать) |  |

1. **Сведения о сетевом оборудовании и объектах мониторинга**

| Параметр | Площадка 1 (ГО) | Площадки |
| --- | --- | --- |
| Общие сведения |
| Локализация (место расположения) |  |  |
| Доступ в Интернет (для лицензирования, обновлений) | Да [ ]  | Нет [ ]  | Да [ ]  | Нет [ ]  |
| Сетевая доступность между площадками (для удалённого сбора событий с источников, прозрачная маршрутизация для сканирования и т.д.) | Да [ ]  | Нет [ ]  | Да [ ]  | Нет [ ]  |
| Пропускная способность/загруженность каналов связи между защищаемыми сегментами (оценка) |  |  |
| Наличие IDS, IPS, межсетевых экранов (МЭ) между сегментами сети | Да [ ]  | Нет [ ]  | Да [ ]  | Нет [ ]  |
| Количество объектов мониторинга |
| Общее количество пользователей |  |  |
| Общее количество сетевых узлов |  |  |
| Общее количество серверов |  |  |
| Общее количество рабочих станций |  |  |
| Общее количество устройств активного сетевого оборудования |  |  |

1. **Функциональные характеристики**

| Тип | Производитель, Название / Модель / Версия | Транспорт и формат логирования (syslog/CEF, Windows Event Log, SNMP, DB) | Среднее кол-во событий в сутки (EPS) | Количество устройств |
| --- | --- | --- | --- | --- |
| Площадка 1 (ГО) | Площадки |
| Операционные системы, централизованная аутентификация |
| Серверные ОС |  |  |  |  |  |
| ОС на рабочих станциях |  |  |  |  |  |
| Службы каталогов (AD / LDAP) |  |  |  |  |  |
| Средства защиты информации |
| Межсетевые экраны |  |  |  |  |  |
| IPS / IDS |  |  |  |  |  |
| Антивирусное ПО |  |  |  |  |  |
| EDR-решения |  |  |  |  |  |
| Proxy |  |  |  |  |  |
| VPN |  |  |  |  |  |
| Email Gateway |  |  |  |  |  |
| «Песочницы» (Network Sandbox) |  |  |  |  |  |
| DLP |  |  |  |  |  |
| Средства анализа защищенности (сканеры уязвимостей) |  |  |  |  |  |
| Системы управления учетными данными (IDM) |  |  |  |  |  |
| Коммутационное и маршрутизирующее оборудование |  |  |  |  |  |
| Другие системы, события от которых необходимо анализировать |
| Платформы виртуализации |  |  |  |  |  |
| Серверы приложений |  |  |  |  |  |
| Flow-протоколы (для NetFlow укажите версию - v5 / v9 / IPFIX) |  |  |  |  |  |
| Другое |  |  |  |  |  |