Техническое задание

в рамках проведения RFI (Request for information) на поставку и внедрение системы **«EDR_защита конечных точек»** для нужд ООО «UMS»

Параметр	
Основные требования	**Значение/Комментарий**
Требуемое исполнение: - ВМ - виртуальная машина	Да
Тип лицензирования: постоянные либо подписочные лицензии	Срок подписки – 3 года., ТП – 3 года.
Количество Дата-центров Заказчика	1
Количество защищаемых рабочих станций	Не менее 1500
Количество защищаемых серверов	Не менее 300
Требуется отказоустойчивость: Active-Active или Active-Standby	Да
Поддержка интеграции с AD	Да
Функциональный требования	
Блокировка вредоносного ПО (Антивирус нового поколения), программ-вымогателей, эксплойтов и атак без использования файлов	Да
Защита устройств с помощью контроля устройств, брандмауэра и шифрования диска	Да
Выявление атак с помощью аналитики на базе ИИ и координация мер реагирования	Да
Управляемое обнаружение и реагирование (MDR)	Да
Управляемая охота за угрозами	Да
Аналитика хоста (Host Insights), поиск уязвимостей и проверка конечных точек для устранения угроз	Да
Быстрое расследование инцидентов с помощью сбора комплексных цифровых доказательств	Да
Интеграции решения по threat intelligence, Slack, отправка Syslog	Да
Применение машинного обучения и UEBA-детекций к данным безопасности	Да
Сбор подробных данных на конечных точках для поддержки глубокой охоты за угрозами в инфраструктуре	Да
Сертификация по стандарту ISO 27001	Да
Предопределенные и настраиваемые правила обнаружения на основе поведения	Да
Наличие специальных правил, которые могут ретроспективно обнаруживать атаки	Да
Обеспечение возможности управления USB-устройствами как минимум для операционных систем Windows	Да
Обеспечение возможности блокирования устройств Bluetooth	Да
Обеспечение возможности запрета печати на указанных устройствах	Да

Возможность интеграции с решением по оркестровке, автоматизации и реагированию на безопасность (SOAR) для анализа инцидентов.	Да
Возможность интеграции с решениями по управлению информацией и событиями безопасности (SIEM)	Да
Обнаружение методов атаки на протяжении всего жизненного цикла атаки, включая обнаружение, управление и контроль, а также фильтрацию	Да
Обеспечение управления доступом на основе ролей для детализированных разрешений	Да
Предоставление API-интерфейсов на основе стандартов, позволяющие интегрировать сторонние инструменты управления и выполнять административные действия	Да
Предоставление настраиваемой панели управления для отображения высокого уровня статуса безопасности и оперативной информации	Да
Тип гипервизора (для исполнения в виде виртуальной машины)	VMWARE
Требования к внедрению/обучению	
Исполнитель выполняет все работы по инсталляции, интеграции и вводу в эксплуатацию решения	
Исполнитель предусматривает разработку проекта	
Исполнитель предусматривает обучение 2 специалистов Заказчика	
Исполнитель обязуется предоставить сертификат Центра Кибербезопасности на предлагаемое решение, либо сертифицировать его на этапе внедрения	