**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

На систему кибербезопасности автоматизированных систем управления технологическим процессом

|  |  |  |
| --- | --- | --- |
| **№**  **п/п** | **Перечень основных данных и требований** | **Основные данные и требования** |
| 1 | Цель проекта | Выполнение работ по внедрению системы кибербезопасности технологических процессов путём защиты от вредоносного ПО на конечных рабочих станциях и серверах технологического сегмента и анализа сетевого трафика в технологических сегментах АСУ ТП. |
| 2 | Перечень работ | * Установка, настройка системы кибербезопасности АСУ ТП; * Проведение специализированных вендорских курсов (*при наличии*); * Проведение вводного инструктажа по эксплуатации системы на базе развернутой системы. |
| 3 | Требование к системе | * Система должна обеспечивать централизованное управление всеми ее компонентами и функционалом мониторинга всех поступающих событий через единый веб-интерфейс без необходимости запуска сторонних приложений, дополнительных интерфейсов, окон или скриптов; * Система должна иметь агентское решение безопасности конечных точек на рабочих станциях и серверах под управлением windows и linux; * Агентское решение безопасности должна быть предназначена для защиты автоматизированных систем управления технологическим процессом с целью минимального воздействия на производительность конечного хоста; * Агентское решение не должно требовать перезагрузки конечного хоста при его установке, обновления баз и конфигураций. * Система должна позволить проводить мониторинг активности конечных устройств в реальном времени; * Система должна иметь различные методы для обнаружения угроз, включая сигнатурный анализ, эвристические методы, поведенческое обнаружение и т.п; * Система должна вести контроль событий, фиксируемых в журналах ОС; * Система должна иметь автоматизацию процедур инвентаризации узлов технологической сети; * Система должна выявлять сетевые атаки и аномальную активность в сетевом трафике; * Система должна обеспечить контроль целостности технологических сегментов, обнаружение новых устройств и сетевых взаимодействий; * Система должна обеспечить контроль уязвимостей ПЛК; * Система должна обеспечить сбор телеметрии (атрибуты конечны узлов, события безопасности об антивирусных инцидентах и т.д.) с рабочих станций и серверов АСУ ТП; * Система должна обеспечить проведение аудита безопасности с помощью OVAL-правил; * Система должна обеспечить обнаружение уязвимостей промышленного ПО; * Система должна иметь инструменты для оперативного реагирования на выявленные угрозы; * Система должна поддерживать возможность разделения дашбордов через пользовательский; * Система должна обеспечивать гибкий процесс управления учетными записями пользователей и их ролями, без необходимости запуска сторонних приложений, дополнительных интерфейсов, окон или скриптов; * Система должна быть локализована на русском и английском языке; * Система должна предоставлять следующие механизмы аутентификации к единой консоли администрирования и управления всеми компонентами:   + Локальная;   + Active Directory;   + LDAP; * Система должна обеспечивать создание и работу с объединенными цепями событий через веб-интерфейс пользователя; * Система должна предоставлять возможность управления, создание аналитических отчетов и правил через веб-интерфейс без необходимости запуска сторонних приложений, дополнительных интерфейсов, окон или скриптов; * Система должна предоставлять удобный и интуитивный интерфейс для быстрой визуализации информации о сети, событиях и инцидентах; * Система должна иметь возможность выгружать отчеты по всем событиям, отчетность должна быть доступа через веб-интерфейс для пользователей решения; * Система должна иметь возможность планирования генерации отчетов в определённый период времени; * Система должна обеспечивать оповещения на основе обнаруженных аномалий в сети; * Оповещение должно осуществляться как веб интерфейсом, так и почтовой рассылкой *(SMTP)*. * Система должна иметь встроенный функционал определения всех активов сети на основе данных из журналов событий, данных с сети *(NetFlow)*, данных об уязвимостях, без дополнительных интерфейсов, окон или скриптов. Вся информация об активах и их свойствах должна храниться в единой базе данных; * Система должна иметь встроенный функционал автоматической классификации и группировки определенных активов в сети без необходимости запуска сторонних приложений, дополнительных интерфейсов, окон или скриптов по следующим параметрам:   + IP адрес;   + Название актива;   + Тип устройства; * Система должна иметь возможность отправки событий в SIEM CEF\Syslog\LEEF. В публичном доступе должен иметься или предоставлен справочник событий. * Система должна иметь возможность передачи выявленных событий и инцидентов ИБ, сведений об активах в SIEM; * Система должна предоставлять стандартную категоризацию событий без предварительных дополнительных настроек; * В системе должен быть реализован интерфейс прикладного программирования *(Application Programming Interface, далее API)*, который обеспечивает доступ к функциям программы для сторонних приложений. В объём поставки должно быть включено ПО и лицензии необходимые для реализации интериации посредствам API. * Система должна иметь возможность шифровать коммуникации между компонентами; * Система должна обеспечить защиту 150 конечных точек *(сервер\рабочая станция)*; * Обработки сетевого трафика NetFlow и\или SNMP и\или SPAN; * Система должна поддерживать режим пассивного анализа трафика с подключением к технологическому сегменту через SPAN-порт или TAP-устройство; * Система должна иметь возможность гибкой настройки мониторинга трафика: включения/отключения отдельных точек мониторинга и технологий анализа трафика; * Система должна поддерживать активный опрос устройств сети по протоколам *(Modbus TCP, S7comm, BECKHOFF, MMS, CIP, SSH, ARP, SNMP, WMI и д.р.)*; * Система должна иметь возможность выявлять и вести оценку рисков *(неправильные настройки, уязвимости, проблемы сетевой архитектуры)*; * Система должна иметь возможность визуализации сетевых взаимодействий в едином веб-интерфейсе * Срок действия технической поддержки должен составлять 1 год; * Система должна поддерживать виртуализацию ПО не ниже VMware vSphere 8; * Программное обеспечение должно быть совместимо со всеми современными протоколами связи локальной сети; * Система должна иметь встроенные инструменты мониторинга работоспособности системы; * Cистема должна быть On-Premise с технической поддержкой со стороны вендора; * Система должна располагаться на локальных серверах КГК, расположенных на территории Кыргызской Республики. |
| 4 | Требования к исполнителю | * Наличие квалифицированных специалистов по внедрению предлагаемого ПО; * Исполнитель должен быть авторизованным партнером компании производителя внедряемого ПО. |
| 5 | Оплата работ | Оплата работ в рамках договора, с учетом всех налогов. |
| 6 | Документация, предоставляемая Исполнителем | * План производства работ; * Список лиц участвующих в работах; * Акт выполненных работ; * Результаты исследования; * Гарантийные обязательства по выполненным работам *(согласовываются между сторонами на стадии заключения договора)*. |