ТЕХНИЧЕСКОЕ ЗАДАНИЕ

На систему сбора событий и управления инцидентами информационной безопасности (*далее – «SIEM» – Security information and event management*).

№ п/п	Перечень основных данных и требований	Основные данные и требования
1	Цель проекта	Выполнение работ по внедрению системы управления и мониторинга событий информационной безопасности, который обеспечивает сбор событий информационной безопасности с узлов информационной инфраструктуры и подсистем, проводит автоматический анализ и корреляцию полученных событий, что позволяет без участия человека на ранней стадии выявлять инциденты информационной безопасности.
2	Перечень работ	• Установка, настройка SIEM; o Взаимодействие (*консультация*) с заказчиком по подключению всех необходимых источников событий; o Нормализация всех нераспознанных событий для не менее 50 источников событий; o Определения перечня инцидентов ИБ которые SIEM должна выявлять; o Разработка не менее 20 отдельных правил\политик выявления инцидентов (*корреляционных правил*); o Доработка не менее 50 уже имеющихся отдельных правил\политик выявления инцидентов (*корреляционных правил*); o Пусконаладочные работы и функциональное тестирование SIEM. • Проведение специализированных вендорских курсов (*при наличии*); • Проведение вводного инструктажа по эксплуатации системы на базе развернутого SIEM; • Разработка технической документации системы (*паспорт системы, общая инструкция по эксплуатации*).
3	**Требование к SIEM:** Требования к пользовательскому интерфейсу	• SIEM должна обеспечивать централизованное управление всеми ее компонентами и функционалом через единый веб-интерфейс без необходимости запуска сторонних приложений, дополнительных интерфейсов, окон или скриптов; • SIEM должна поддерживать возможность разделения дашбордов через пользовательский интерфейс для использования во внедрениях SOC (Security Operations Center); • SIEM должна обеспечивать гибкий процесс управления учетными записями пользователей и их ролями, без

		необходимости запуска сторонних приложений, дополнительных интерфейсов, окон или скриптов; • Компоненты управления SIEM должны быть локализованы на русском и английском языке; • SIEM должна предоставлять следующие механизмы аутентификации к единой консоли администрирования и управления всеми компонентами: o Локальная; o Active Directory; o LDAP. • SIEM должна обеспечивать создание и работу с объединенными цепями событий через веб-интерфейс пользователя на основе информации о: информация из журналов событий (logs) и выявленных инцидентов без необходимости запуска сторонних приложений, дополнительных интерфейсов, окон или скриптов; • SIEM должна предоставлять возможность управления системой, создание аналитических отчетов и правил через веб-интерфейс без необходимости запуска сторонних приложений, дополнительных интерфейсов, окон или скриптов; • SIEM должна предоставлять удобный и интуитивный интерфейс для быстрой визуализации информации о сети, событиях и инцидентах.
4	**Требование к SIEM:** Отчёты и оповещение	• SIEM должна иметь возможность выгружать отчеты по всем событиям, отчетность должна быть доступа через веб-интерфейс для пользователей решения; • SIEM должна иметь возможность самостоятельной настройки отчетности и создание собственных отчетов пользователем; • SIEM должна иметь возможность планирования генерации отчетов в определённый период времени; • SIEM должна иметь возможность генерации новых отчетов пользователем, а также мастер создания отчетов; • SIEM должна иметь отчеты по определенным требованиям стандартов, а также лучших практик (NIST, CoBIT, ISO); • SIEM должна предоставлять отчёты за определенный период времени по разным сегментам и системам в сети; • SIEM должна предоставлять возможность автоматического распределения отчетов; • SIEM должна предоставить возможность создания отчетов на основе информации о: уязвимости инфраструктуры, данные о конфигурации устройств безопасности (систем предотвращения вторжение (IPS), маршрутизаторов и брандмауэров (firewall)), информации из журналов событий (logs), информация из сети потоков (NetFlow) и выявленных инцидентов без необходимости запуска

		сторонних приложений, дополнительных интерфейсов, окон или скриптов. Вся информация должна собираться, обрабатываться и храниться в единой базе данных системы для оперативного получения необходимой информации и уменьшения нагрузки и сложности процесса управления системой; • SIEM должна обеспечивать оповещения на основе обнаруженных аномалий и поведенческого анализа и изменений; • SIEM должна обеспечивать оповещение по установленным политикам; • SIEM должна извещать, администратора, если перестали поступать журналы событий с устройства в сети (например, нет событий от сервера в течение определённого времени); • Оповещение должно осуществляться как веб интерфейсом, так и почтовой рассылкой (*SMTP*).
5	**Требование к SIEM:** Работа с данными и их нормализация	• SIEM 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; • SIEM 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: o IP адрес; o Название актива; o Операционная система; o Найденные Сервисы; o Пользователь. • SIEM должна поддерживать расширенную таксономию пользователей для событий и полей. Пользователь должен иметь возможность присваивать событиям любые имена; • SIEM должна иметь возможность получения и обработки потоков сетевого трафика (NetFlow); • SIEM должна поддерживать стандартные методы сбора журналов событий (например, syslog, WMI, JDBC, SNMP, Checkpoint LEA, и др.); • SIEM должна поддерживать безагентный сбор журналов событий везде, где это возможно; • SIEM должна предоставлять стандартную категоризацию событий без предварительных дополнительных настроек; • SIEM должна иметь возможность сохранять информацию о событиях, как в исходном виде, так и в нормализованном виде для использования в дальнейших расследованиях;

		• SIEM должна иметь возможность обрабатывать и нормализовать данные с полей, которые не поддерживаются изначально и не предоставляются с настройками out of the box; • SIEM должна обеспечивать анализ событий в режиме реального времени; • SIEM должна обеспечивать анализ событий в течение определенного периода времени; • SIEM должна обеспечивать фильтрацию, а также показывать через интерфейс события в режиме реального времени, где пользователь может сразу же применять политики и фильтры; • SIEM должна обеспечивать корреляцию информации с разных источников, которые никак не взаимодействуют между собой; • SIEM должна предоставлять возможность сбора, анализа и корреляции данных о журналах событий и по инфраструктуре, а также автоматизацию безопасности сети. • SIEM должна автоматически определять и при возможности добавлять нестандартные источники событий, которые были подключены пользователем • SIEM должна предоставлять возможность перевода параметров поиска по всем нормализованным и ненормализованным данным с использованием графического интерфейса системы; • SIEM должна предоставлять возможность ручной загрузки событий для дальнейшего анализа корреляционными правилам с целью выявления потенциальных угроз.
6	**Требование к SIEM:** Реагирование на угрозы	• SIEM должна иметь не менее 100 предустановленных корреляционных правил; • SIEM должна иметь возможность расширения количества корреляционных правил (например, для выявления новых угроз), отчетов и встроенных поисков за счет установки приложений, которые должны быть проверены производителем системы; • SIEM должна предоставлять возможность визуализации типичных угроз и построения правил для их обнаружения согласно MITRE ATT & CK Framework; • SIEM должна предоставлять возможность пользователю оценивать уровень покрытия правилам обнаружения угроз известных тактик и техник по MITRE ATT & CK Framework; • В целях эффективного реагирования на инциденты, SIEM должна иметь возможность дооснащения модулем искусственного интеллекта (*AI*) от производителя.

7	**Требование к SIEM:** Совместимость	• SIEM должна поддерживать интеграцию (*на уровне уведо*млений) с другими системами безопасности и оповещения, функционирующих в сети; • SIEM должна иметь возможность коррелировать информацию из систем сканирования уязвимостей сторонних производителей; • SIEM должна иметь возможность расширения функционала за счет установки приложений\компонентов, которые должны быть проверены производителем системы; • SIEM должна поддерживать возможность создания пользователем собственных моделей машинного обучения; • Все компоненты системы должны быть частью единой системы управления и мониторинга событий информационной безопасности; • Развертывание всех модулей системы должно обеспечиваться с единого образа ПО; • SIEM должна гарантировать актуальность данных, собираемых и обрабатываемых в единой базе данных - обеспечивать обработку и корреляцию данных из журналов событий (*logs*) с задержкой не более 1 секунды после получения данных системой от источника событий.
8	**Требование к SIEM:** Общие требования к системе	• SIEM должна иметь возможность шифровать коммуникации между компонентами; • SIEM должна обеспечивать процесс сбора, хранения и обработки информации о журналах событий, активов через единое виртуальное устройство (virtual appliance), имеющее единый постоянный IP адрес в локальной сети без необходимости запуска и использования сторонних приложений, баз данных, дополнительных интерфейсов, окон или скриптов или других виртуальных устройств; • SIEM должна обеспечивать автоматическое обновление конфигураций без дополнительных временных затрат со стороны пользователя системы путем автоматической загрузки их с сервера обновлений, что может находиться в сети интернет, или в локальной сети организации; • SIEM должна поддерживать отказоустойчивое внедрение; • SIEM должна обеспечить работу отдельных компонентов системы, при выходе из строя любой части системы. (Например, центральная консоль выходит из строя, но лог коллекторы продолжают функционировать); • SIEM должна иметь встроенный процесс анализа своего состояния и оповещать пользователя при возникновении проблем; • SIEM должна давать возможность развернуть при необходимости платформу для координации и

		автоматизации процессов реагирования расследование инцидентов от производителя Системы; • SIEM должна обеспечивать целостность собранной информации; • SIEM должна предоставлять прозрачное получение, агрегирование, сортировку, фильтрацию и аналитику данных по всем разнесенным компонентам системы; • SIEM должна обеспечивать встроенный функционал определения известных устройств и их инвентаризации по классам систем (например, почтовые серверы, серверы баз данных и др.); • SIEM должна иметь функционал поведенческого анализа пользователей (*UBA*): o Модуль поведенческого анализа должен предоставлять не менее 50 корреляционных правил; o Модуль поведенческого анализа должен использовать модели машинного обучения и не нуждаться в дополнительном лицензировании; o Модуль поведенческого анализа не должен содержать ограничений по количеству учетных записей; o Модуль поведенческого анализа должен эффективно использовать имеющиеся в системе данные - журналы событий и сетевые коммуникации; o Модуль поведенческого анализа должен автоматически определять уровень риска активности пользователей. • SIEM должна иметь возможность выявления угроз на уровне DNS (использование алгоритмов генерации доменных имен (DGA), передача данных через DNS запросы (DNS Tunneling), выявления попыток доступ к запасных доменных имен (DNS Squatting) на основании данных от DNS серверов или других систем. • SIEM должна иметь возможность масштабироваться и расширять функционал (*при добавлении новых устройств, офисов, приложений в сети заказчика*) для соответствия требованиям бизнеса;
9	**Требование к SIEM:** Резервное копирование и хранение данных	• SIEM должна иметь функционал автоматического процесса резервного копирования и возможность восстановления с графического интерфейса пользователя; • SIEM должна иметь систему сбора журналов событий и их архивации, которая поддерживает как кратковременное хранение (online), так и долгосрочное (offline) хранение журналов событий; • SIEM должна обеспечивать рациональное использование хранилищ данных;

		• SIEM должна предоставлять доступ ко всей информации о событиях на протяжении длительного периода времени (например, 36 месяцев) для дальнейших расследований. • События и\или источники событий, выходящие за рамки лимита лицензий, должны храниться и обрабатываться в порядке очереди до появления освободившихся лицензий.
10	Лицензии и техническая поддержка	• Количество лицензий будет зависеть от типа лицензирования: либо 3000 EPS, либо 1000 хостов (*серверные ОС, сервисы,ПК, коммутаторы и т.п.*); • Лицензия на программное обеспечение SIEM должна быть бессрочной; • Срок действия технической поддержки должен составлять 1 год; • По истечении срока действия технической поддержки SIEM, следующий функционал должен продолжать работу: o Вход в консоль SIEM; o Изменение конфигурации SIEM; o Агрегация событий; o Создание и изменение корреляционных правил; o Работа уже имеющихся корреляционных правил; o Нормализация событий; o Подключение новых источников событий.
11	Требования к исполнителю	• Опыт внедрения предлагаемого ПО; • Опыт реализации проектов в горнорудной промышленности будет являться преимуществом при отборе исполнителя; • Наличие квалифицированных специалистов по внедрению предлагаемого ПО; • Исполнитель должен быть авторизованным партнером компании производителя внедряемого ПО;
12	Оплата работ	Оплата работ в рамках договора, с учетом всех налогов.
13	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);