## Требования к программному обеспечению оперативного мониторинга состояния информационной безопасности (SIEM)

### Общие требования

Система должна иметь заключение о соответствии требованиям к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, утвержденным приказом ФСБ России от 6 мая 2019 г. №196.

### Требования к оборудованию

* Компоненты системы должны поддерживать установку как на физических, так и на виртуальных машинах.
* Основные компоненты (модули, отвечающие за сбор событий, корреляцию, хранение событий) должны поддерживать установку на операционной системе семейства Linux:
  + Astra Linux Special Edition 1.7.1-1.7.4;
  + Oracle Linux версии 8.6, 8.7, 9.2.
* Система должна обеспечивать высокую производительность и поддерживать прием и обработку потока в размере до 300 000 событий в секунду (EPS) на одном сервере.
* Для хранения событий должна использоваться колоночная база данных для обеспечения высокой скорости поиска.

### Требования к архитектуре системы

* Система должна поддерживать горизонтальное масштабирование ключевых ее компонентов: коллектора, коррелятора и хранилища событий без необходимости приобретения дополнительных лицензий на ПО.
* Сетевое взаимодействие всех компонентов SIEM должно выполняться по шифрованным каналам связи
* Компоненты системы должны поддерживать установку в распределённых и изолированных сетях без необходимости доступа к сети Интернет.
* Система должна поддерживать возможность сбора событий из изолированных сегментов сети через дата-диод, в том числе при отсутствии возможности передачи событий с использованием UDP-пакетов.
* Система должна обеспечивать централизованное управление посредством веб-консоли без установки дополнительного ПО на АРМ администратора.
* Система должна поддерживать мультитенантность, позволяя в рамках единой инсталляции создавать независимые тенанты с возможностью разграничения прав доступа пользователей системы к событиям, инцидентам, правилам корреляции, нормализации, а также определенным настройкам системы по отношению к разным тенантам.
* Система должна обеспечивать возможность централизованного обновления конфигурации или перезапуска компонентов, в том числе форсированного.
* Система должна поддерживать гибкую настройку маршрутизации событий между компонентами.
* Система должна обеспечивать режим работы отказоустойчивого кластера для всех компонентов с «горячим» переключением (High Availability);
* Система должна поддерживать работу с несколькими независимыми кластерами хранилища событий для возможности организации гибких схем географически распределенных систем.
* Архитектура решения должна обеспечивать возможность развертывания в географически распределенной инфраструктуре, как минимум в следующем объёме:
  + Система должна поддерживать возможность передачи определенных событий из удалённых офисов на центральные корреляторы;
  + Возможность локального сбора, нормализации, агрегации, фильтрации и обогащения событий ИБ в удаленных офисах за счет установки локального коллектора системы.
* Система должна поддерживать поиск по событиям в удалённых офисах из центрального узла системы.
* Система должна предоставлять RESTful API для управления активами, активными листами, работы с зарегистрированными базовым и корреляционным событиям ИБ: поиск, получение контекстной информации по базовым и корреляционным событиям ИБ, управление статусом обработки.
* Система должна поддерживать автоматическое обновления правил нормализации и правил корреляции, выпускаемых производителем. Должна быть реализована возможность ревизии изменений оператором после получения оповещения о новых доступных ресурсах. Система должна поддерживать обновление в том числе без прямого доступа к интернету с использованием механизма «зеркала обновления».

### Требования к сбору, анализу и хранению событий

* Система должна обеспечивать как активный, так и пассивный сбор событий с источников данных.
* Система должна обеспечивать унифицированную модель данных.
* Система должна обеспечивать сбор событий посредством следующих транспортов:
* Netflow (v9, v5), sFlow;
* IPFIX;
* TCP, UDP;
* HTTP;
* WEC, WMI;
* SNMP, SNMP-trap;
* FTP, NFS, filereader;
* API;
* SQL – выполнение запросов, обработка результатов (с поддержкой ID-based и Time-Based таблиц);
* Kafka, nats-jetstream.
* Система должна предоставлять централизованный интерфейс управления списком сборщиков(коллекторов) событий.
* Система должна поддерживать возможность опциональное сохранения исходного (raw) события. Настройки должны предусматривать как безусловное сохранение события, так и сохранение только в случае ошибок разбора события.
* Система должна поддерживать возможность добавления пользовательских типов источников событий и соответствующей настройки правил разбора и нормализации.
* Система должна обеспечивать создание пользовательских парсерсов на основе поддерживаемых форматов и протоколов сбора данных.
* Система должна обеспечивать возможность написания правил нормализации из веб-интерфейса системы для разбора событий, в том числе посредством регулярных выражений и возможностью проверки синтаксиса их написания на примере исходного события.
* Система без дополнительных настроек разбора (нормализации) должна поддерживать получение событий в форматах Syslog, CEF.
* Система должна обеспечивать возможность создавать пользовательские поля для реализации произвольной пользовательской таксономии. Должно быть доступно создание полей следующих типов:
  + Строковый
  + Числовой
  + С плавающей точкой
  + Массив строк
  + Массив чисел
  + Массив чисел с плавающей точкой
* Система должна поддерживать возможность последовательного иерархического разбора (нормализации) событий.
* Компонент сбора событий (коллектор) должен обеспечивать буферизацию событий на локальном диске на случай временной недоступности получателей событий, а также автоматическую пересылку буферизованных событий после восстановления соединения. Размер буфера для хранения событий должен быть настраиваемым.
* На этапе первоначальной обработки полученных событий компонент сбора (коллектор) должен обеспечивать:
  + Нормализацию событий;
  + Фильтрацию событий;
  + Агрегацию событий (с возможностью применения математических функций);
  + Модификацию/мутацию событий;
  + Коррекцию времени событий;
  + Потоковое обогащение событий в соответствии с перечнем источников обогащения (см. ниже).
* Система должна обеспечивать возможность мониторинга поступления событий от источников с отслеживанием количества событий в указанный промежуток времени и автоматическим оповещением на электронную почту в случае отклонения от заданных параметров мониторинга для каждого из источников в частности;
* Система должна поддерживать разделение уровней хранения событий («горячий» и «холодный» уровни). При этом данные должны быть прозрачно доступны из интерфейса поиска без необходимости дополнительно загружать события из «холодного» хранения либо разделять поиски по типам и срокам хранения. Параметры сроков хранения должны определяться пользователем в графическом интерфейсе системы.
* Возможность выгрузки событий в архив длительного хранения.
* Система должна поддерживать логическое разделение общего объема хранилища на группы с разными сроками хранения событий и возможностью распределять события по этом группам в соответствии с пользовательскими фильтрами.
* Система должна обеспечивать возможность поиска по базе событий на основе произвольного поиска по базе событий с помощью конструктора запросов;
* Система должна обеспечивать возможность поиска по базе событий на основе SQL-like языка запросов с возможностью проведения группировок и вычислительных операций;
* Система должна обеспечивать возможность вывода статистики полей по базе событий;
* Система должна поддерживать импорт/экспорт контента и ресурсов: правил корреляции, парсеров, коннекторов и т.д.

### Требования к функциям обогащения событий

* Система должна поддерживать обогащение событий как на коллекторах (на этапе сбора и обработки событий), так и на корреляторе (для обогащения коррелированных событий)
* Должна обеспечиваться возможность потокового обогащения событий посредством сопоставления событий с потоками данных об угрозах путем интеграции с платформой Threat Intelligence. Данные о найденных индикаторах компрометации должны сразу включаться в базовые события с возможностью дальнейшего использования в рамках корреляции.
* Лицензия системы должна включать возможность подключить к KUMA потоки данных об индикаторах компрометации как компании-производителя, так и сторонних поставщиков (OSINT-источники и по стандартному протоколу TAXII)
* Потоки данных производителя системы должны включать:
  + ransomware url - URL-адреса и маски, которые относятся к «шифровальщикам»
  + botnet url - URL-адреса и маски для обнаружения командных центров и веб-ресурсов, относящихся к ботнет сетям
  + malicious url - вредоносные URL-адреса и маски для обнаружения вредоносных веб-ресурсов
  + phishing url - фишинговые URL и маски для обнаружения фишинговых веб-ресурсов
  + ip reputation - содержит подозрительные и вредоносные IP-адреса
* Cистема должна поддерживать возможность выполнять обогащение конкретных событий по запросу аналитика в репутационный сервис, доступный онлайн. запрос должен выполняться по доменам, веб-адресам, IP-адресам и хешам файлов и выполнять обогащение сведениями об опасных и вредоносных, так и легитимных объектов.
* Система должна поддерживать следующих механизмы и источники для обогащения событий:
  + Сведения об активах и группах информационных активов, имеющиеся во встроенной базе активов;
  + Сведения о пользователях и группах, имеющиеся в службе каталогов Active Directory;
  + DNS;
  + База географических данных IP-адресов;
  + Создаваемые пользователем словари;
  + Сведения о часовом поясе источника событий;
  + Контекстная информация Threat Intelligence (cведения об индикаторах компрометации и соответствующем контексте хэши файлов, URL-адреса, внешние IP-адреса).
* Система должна поддерживать возможность обогащения событий, содержащих IP-адреса, географическими данными на основе загруженных списков геоданных.
* Система должна поддерживать возможность использования геоданных, полученных из сервисов MaxMind и IP2Location.
* Система должна поддерживать создание пользовательских словарей для обогащения событий и возможность их наполнения через web-интерфейс и/или API.
* Словари, используемые для обогащения, должны поддерживать возможность добавления не менее 50000 записей.
* Система должна поддерживать возможность обогащения событий информацией о смещении времени источника событий относительно всемирного координированного времени (UTC).

### Требования к функциям корреляции событий

* Система должна обеспечивать потоковую корреляцию событий ИБ в режиме близком к режиму реального времени.
* Компонент корреляции должен поддерживать применение активных списков (Active List / Reference Set) в правилах корреляции.
* Для активных списков должны поддерживаться как минимум следующие операции:
  + Создание, удаление списков пользователем через UI;
  + Проверка существования, добавление, изменение и удаление строк как результат работы правила корреляции;
  + Импорт и экспорт списков в табличном формате;
  + Поддержка настраиваемого времени жизни (TTL) для записей в активных списках;
  + Поддержка возможности изменения набора колонок без пересоздания активного списка.
* Система должна поставляться с набором предустановленных правил корреляции, созданных на основе исследований актуальных угроз и способов атак, разработанных на базе матрицы MITRE ATTACK;
* Система должна поддерживать возможность создания собственных правил корреляции. При этом должно быть доступно как написание условий фильтров и корреляционных правил в виде кода, так и в графическом редакторе.
* Система должна поддерживать возможность тестирования правил корреляции на исторических данных без установки дополнительных модулей.
* Система должна поддерживать многоуровневое применение правил корреляции, при которой результаты срабатывания одних правил корреляции являются источниками для следующих правил корреляции.
* Правила корреляции в Системе должны поддерживать:
  + Корреляцию по количественному признаку;
  + Корреляцию по последовательности событий;
  + Операции выделения фрагментов события (substring, regexp и т.д.);
  + Автоматическое оповещение при срабатывании правила корреляции;
  + Корреляцию по глобальным и локальным переменным.
* Система должна автоматически приоритизировать выявленные угрозы ИБ как с учётом уровня критичности правила корреляции, так и с учетом критичности и количества затронутых информационных активов.
* Система должна обеспечивать возможность написания правил корреляции с учетом вхождения актива в ту или иную группу.
* Система должна поддерживать автоматическое объединение скоррелированных событий по гибко настраиваемым пользовательским фильтрам.
* Глобальные переменные корреляции должны действовать в пределах коррелятора, на котором они объявлены, и при применениях в правилах корреляции, должны иметь возможность принимать различные значения в рамках каждого условия срабатывания правила корреляции (селектора).
* Локальные переменные корреляции должны действовать только в рамках корреляционного правила и условия срабатывания правила корреляции (селектора) в котором они объявлены.
* Переменные корреляции должны поддерживать следующие функции:
  + Получение информации из активного листа о значении в указанном столбце;
  + Получение информации о значении в указанном столбце словаря;
  + Возврат числа символов в строке;
  + Перевод символов в строке в нижний регистр;
  + Перевод символов в строке в верхний регистр;
  + Добавление символов в конец строки;
  + Добавление символов в начало строки;
  + Возврат подстроки из строки по координатам начала и конца подстроки;
  + Удаление из начала и/или конца строки указанных символов/подстроки;
  + Замена в строке всех вхождений последовательности символов А на последовательность символов B;
  + Замена в строке последовательности символов, удовлетворяющих регулярному выражению, на последовательность символов и группы захвата регулярного выражения;
  + Получение из исходной строки результата, удовлетворяющего условию регулярного выражения;
  + Получение временной метки в формате epoch;
  + Получение атомарных представлений времени (в виде год, месяц, день, час, минута, секунда, день недели) из полей и переменных cо временем в формате epoch;
  + Преобразование времени из формата RFC3339 в формат epoch и наоборот;
  + Округление времени в формате epoch (до секунд/минут/часов/суток);
  + Получение интервала времени между двумя метками времени в формате epoch (в секундах/минутах/часах/днях);
  + Основные математические операции:
    - Сложение;
    - Вычитание;
    - Умножение;
    - Деление;
    - Деление по модулю;
    - Округление числа (в большую/меньшую сторону);
    - Получение числа по модулю;
    - Возведение в степень.

### Требования к функциям реагирования

* Система должна поддерживать вызов функций автоматизированного реагирования в результате срабатывания правил корреляции.
* Система должна поддерживать следующие механизмы реагирования:
  + Автоматический запуск пользовательских скриптов (серверных);
  + Принудительный запуск внеочередной проверки на вирусы или обновления баз через сервер управления средств защиты конечных точек как в ручном режиме (из карточки актива), так и автоматически (при срабатывании правила корреляции);
  + Принудительный запуск внеочередного обновления баз через сервер управления средств защиты конечных точек как в ручном режиме (из карточки актива), так и автоматически (при срабатывании правила корреляции);
  + Реагирование с использованием возможностей EDR-агентов как в ручном режиме (из карточки актива), так и автоматически (при срабатывании правила корреляции). Должны быть доступны следующие действия:
    - Сетевая изоляция хоста с настройкой исключений;
    - Запуск произвольных команд на хосте и получение результатов выполнения;
    - Создание правила запрета на основе параметров событий, получаемых SIEM
  + Реагирование с использованием возможностей средств защиты веб-трафика автоматически (при срабатывании правила корреляции). Должны быть доступны следующие действия:
    - Блокировка по e-mail;
    - Блокировка по IP.
  + Реагирование с использованием возможностей средств антивирусной защиты и фильтрации спама для почтовых серверов автоматически (при срабатывании правила корреляции). Должны быть доступны следующие действия:
    - Блокировка по URL;
    - Блокировка по IP;
    - Блокировка по DOMAIN.
  + Реагирование с использованием возможностей решений для защиты инфраструктуры промышленных предприятий как в ручном режиме (из карточки актива), так и автоматически (при срабатывании правила корреляции). Должно быть доступно изменение статуса актива.
  + Управление учетными записями в Active Directory как в ручном режиме (из карточки учетной записи), так и автоматически (при срабатывании правила корреляции). Должны быть доступны следующие действия:
    - Добавление и удаление учетной записи из группы;
    - Сброс пароля учетной записи;
    - Блокировка учетной записи.
  + Управление уровнем осведомленности сотрудников путем назначения соответствующих курсов из карточки учетной записи.

### Требования к управлению сведениями об активах

* Система должна обеспечивать сбор и автоматическое обновление и хранение во встроенной базе данных в том числе следующей инвентаризационной информации об информационных активах:
  + IP
  + MAC
  + FQDN
  + Перечень установленного ПО
  + Информация об актуальных уязвимостях ПО
  + Информация об аппаратном обеспечении
  + Категория КИИ
  + Дата последнего обновления защиты
  + Статус защитного ПО, установленного на активе
* Система должна предоставлять возможность добавлять пользовательские поля в карточку актива;
* Система должна поддерживать следующие механизмы наполнения и обновления встроенной базы информационных активов:
  + Автоматической сбор и обновление информации посредством интеграции с сервером управления от средств защиты конечных точек;
  + Автоматический сбор и обновление информации посредством интеграции с средством защиты промышленных/технологических сетей;
  + Ручное добавление отчетов по информации об активах и уязвимостях от сканера уязвимости;
  + Ручное добавление или редактирование информации об активах через графический интерфейс Системы;
  + Импорт активов через REST API.
* Система должна поддерживать создание пользовательских групп (категорий) активов;
* Система должна обеспечивать возможность автоматической категоризации активов на основе одного или комбинации признаков: ОС, IP адресации, FQDN, наличия CVE ID и версии ОС.
* При задании условий автоматической категоризации активов система должна поддерживать логические операторы И, ИЛИ, НЕ, а также их группировку.
* При задании условий автоматической категоризации активов система должна обеспечивать возможность тестирования заданных условий по имеющейся базе информационных активов.
* Система должна поддерживать возможности поиска по активам, сохраненных во встроенной базе данных.
* Для активов, импортированных из KSC или KICS, должен поддерживаться механизм архивирования, при котором активы KUMA помечаются как архивные и по истечении заданного пользователем периода и могут быть удалены, если агенты на этих активах более не подключаются к KSC или KICS.
* Система должна поддерживать функцию аудита активов и отслеживать следующие события:
  + Добавление актива в систему;
  + Изменение параметров актива (имя, IP-адрес, MAC-адрес, FQDN, ОС);
  + Удаление актива из системы;
  + Добавление сведений об уязвимости в актив;
  + Удаление/изменение сведений об уязвимости актива;
  + Изменение (добавление/удаление) категории актива

### Требования к функциям работы с инцидентами

* Система должна обеспечить формирование карточки события обнаружения.
* Карточка должна поддерживать следующие возможности:
  + Изменение приоритета инцидента;
  + Назначение инцидента на выбранного аналитика;
  + Переход к связанным базовых событий из карточки инцидента;
  + Автоматическое ведение журнала изменений статуса и выполненных действий карточки;
  + Отображение информационных активов, пользователей, связанных с инцидентом, а также доступной контекстной информации о них;
  + Выделение информации о связанных с событием обнаружения активах и пользователях с указанием их ценности;
  + Привязка дополнительных событий вручную для анализа причины инцидента;
* Должна быть реализована возможность объединения нескольких событий корреляции в единый инцидент, как в ручном режиме, так и автоматическом: на основе временного диапазона формирования события корреляции, на основе учетной записи пользователя.
* Должна быть реализована возможность ручной привязки дополнительной информации к инциденту - по пользователям, активам, событиям корреляции с возможности классификации инцидента.

### Требования к визуализации и отчётности

* Система должна предоставлять инструменты визуализации (дашборды) и отчётности для следующих объектов:
  + События;
  + Алерты
  + Инциденты;
  + Активы;
  + Источники событий;
  + Активные листы.
* Система должна поставляться с предустановленным набором графических панелей (дашбордов) и отчётов.
* Система должна поддерживать возможность создания пользовательских шаблонов и правил уведомлений о событиях и инцидентах.
* Система должна обеспечивать отображение следующих данных по инцидентам в графическом формате (дашборды):
  + созданные инциденты;
  + закрытые инциденты за период;
  + незакрытые инциденты по критичности;
  + распределение инцидентов;
  + инциденты по уровню критичности;
  + затронутые активы и группы активов;
  + источники событий с наибольшим количеством инцидентов;
  + правила корреляции с наибольшим количеством инцидентов;
  + распределение инцидентов по тенантам (со сравнением с прошлым периодом);
  + распределение инцидентов по времени обнаружения (first seen);
  + распределение количества затронутых инцидентами активов по тенантам.
* Система должна обеспечивать отображение следующих данных по событиям в графическом формате (дашборды):
  + часто встречаемые внутренние IP-адреса в Netflow;
  + часто встречаемые внешние IP-адреса в Netflow;
  + статистика объемов трафика относительно портов;
  + статистика по источникам с наибольшим количеством событий.
* Система должна поддерживать возможность создания пользовательских дашбордов и шаблонов отчетов.
* Система должна поддерживать создание графических панелей (дашбордов) на основе пользовательских запросов к хранилищу событий.
* Формирование и настройка пользовательских графических панелей (дашбордов) или отчётов должно полностью выполняться в графическом веб-интерфейсе.
* Система должна обеспечивать возможность формирования отчетов из состава имеющихся шаблонов:
  + по источникам;
  + по инцидентам;
* Система должна обеспечивать построение отчетов по инцидентам со следующей информацией:
  + количество активных инцидентов;
  + количество нераспределенных инцидентов;
  + распределенные инциденты по времени;
  + последние инциденты по времени;
  + количество инцидентов с распределением по уровню критичности;
  + количество инцидентов по исполнителям;
  + количество инцидентов с распределением по статусу;
  + затронутые активы и группы активов;
  + источники событий с наибольшим количеством инцидентов;
  + правила корреляции с наибольшим количеством инцидентов;
  + затронутые учетные записи;
  + на основе произвольного поиска по базе событий с помощью конструктора.
* Система должна обеспечивать построение отчетов по источникам со следующей информацией:
  + часто встречаемые внутренние IP-адреса в Netflow;
  + часто встречаемые внешние IP-адреса в Netflow;
  + статистика объемов трафика относительно портов;
  + статистика по источникам с наибольшим количеством событий.
* Система должна обеспечивать возможность отправки отчетов по почте, размещения отчёта на сетевом хранилище и публикации отчёта через консоль управления системой.
* Система должна поддерживать рассылку отчетов по настраиваемому расписанию.
* Система должна предоставлять возможность экспорта отчетов в формате HTML, CSV, раздельный CSV, XLSX.

### Требования к мониторингу производительности

* Система должна обеспечивать сбор и хранение метрик производительности всех компонентов Системы.
* Метрики производительности должны отображаться в графическом интерфейсе Системы.
* Система должна собирать, хранить и отображать как минимум следующие метрики производительности:
  + Потребление памяти;
  + Количество обрабатываемых (входящих в компонент и исходящих из компонента) событий в секунду с разделением по источникам;
  + Задержки времени (latency) на каждом этапе обработки событий;
  + Параметры работы с активными списками (количество запросов, задержки);
  + Параметры работы с внешними системами (количество запросов, задержки).
* Система должна поддерживать передачу метрик производительности во внешние системы мониторинга.
* Система должна поддерживать возможность отправки почтовых уведомлений при нарушении определенных пороговых значений.

### Требования к безопасности

* Система должна обеспечивать разграничение прав доступа на основе ролевой модели;
* Система должна регистрировать события доступа и значимых изменений конфигурации;
* Система должна поддерживать аутентификацию и авторизацию с использованием следующих механизмов:
  + Локальная база учётных данным (по логину-паролю) пользователей;
  + AD, ADFS, FreeIPA.
* Система должна иметь встроенные механизмы противодействия попыткам подбора пароля.

## Требования к эксплуатационной документации

* Эксплуатационная документация Системы должна включать Руководство пользователя и Руководство Администратора.
* Документация, поставляемая в комплекте с Системой, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства.

## Требования к технической поддержке

Техническая поддержка программного обеспечения должна соответствовать следующим требованиям:

* предоставляться на русском языке сертифицированными специалистами производителя решения на всей территории Республики Казахстан по инцидентам;
* web-сайт производителя должен быть на русском языке, иметь пополняемую базу знаний, а также форум пользователей программных продуктов;
* предоставлять возможность использования персональной учетной записи пользователя для создания, обновления и мониторинга инцидентов;
* предоставлять техническую поддержку и консультации по решению инцидентов в процессе установки, конфигурирования и функционирования продукта;
* определять приоритет запроса к службе технической поддержки на основе влияния проблемы на бизнес-процессы;
* присваивать более высокий приоритет запросам пользователей расширенной технической поддержки относительно стандартных запросов;
* регулярно информировать о промежуточных результатах и ходе решения запросов;
* предоставлять возможность предъявления претензий и жалоб на качество обслуживания на уровень руководителя технический поддержки регионального офиса или менеджера по работе с корпоративными клиентами;

Техническое консультирование по вопросам эксплуатации продукта и приём запросов на устранение негативных последствий инцидентов должно обеспечиваться посредством:

* Предоставления доступа Пользователю к Интернет-Порталу технической поддержки с возможностью размещения запросов в режиме 24x7x365 (круглосуточно, включая выходные и праздничные дни);
* Приёма запросов по телефону выделенной приоритетной линии в режиме 24x7x365 для запросов уровня критичности 1;
* Приёма запросов по телефону выделенной приоритетной линии по рабочим дням с 10:00 по 18:30 (время г.Алматы) для запросов уровня критичности 2, 3 и 4;
* Приёма запросов по электронной почте в режиме 24x7x365 (круглосуточно, включая выходные и праздничные дни) в случае невозможности создания запроса через Интернет- Портал;

Время реакции должно обеспечиваться согласно уровню критичности:

|  |  |  |
| --- | --- | --- |
| **Уровень критичности** | | **Время реакции не более:** |
| Уровень критичности 1 | Критический | 2 рабочих часа |
| Уровень критичности 2 | Высокий | 6 рабочих часа |
| Уровень критичности 3 | Средний | 8 рабочих часов |
| Уровень критичности 4 | Низкий | 10 рабочих часов |

Уровни критичности инцидентов, относящихся к продукту должны соответствовать следующему описанию:

**Уровень критичности 1 (критический)** означает критическую проблему с Продуктом, влияющую на непрерывность бизнеса Пользователя посредством прерывания работоспособности Продукта или операционных систем Пользователя, или вызывающую потерю данных, установку стандартных настроек Пользователя в небезопасный режим или возникновение других проблем с безопасностью, при этом обходное решение отсутствует.

Перечень инцидентов, связанных с Продуктом и соответствующих Уровню критичности 1, включает в себя следующие инциденты:

* вся локальная сеть (или критичная часть сети) не работает, что прерывает основные бизнес- процессы.

**Уровень критичности 2 (высокий)** означает проблему высокого уровня критичности, вызывающую воздействие на функциональность Продукта, но не вызывающую повреждение/ потерю данных или прерывание работоспособности программного обеспечения. Уровень критичности 1 рассматривается, как Уровень критичности 2, когда известно обходное решение.

Перечень инцидентов, связанных с Продуктом и соответствующих Уровню критичности 2, включает в себя следующие инциденты:

* продукт полностью выведен из строя, но непрерывность основных бизнес-процессов не нарушается.

**Уровень критичности 3 (средний)** означает некритичную проблему или запрос на обслуживание, не затрагивающие функциональность Продукта.

Перечень инцидентов, соответствующих Уровню критичности 3, включает в себя следующие инциденты:

* продукт частично выведен из строя (работает несоответствующим образом), но другое программное обеспечение Заказчика не выведено из строя в результате работы Продукта.

**Уровень критичности 4 (низкий)** означает другие некритичные запросы на обслуживание. Все инциденты, не упомянутые выше, относятся к этому уровню критичности.

Дополнительные требования к технической поддержке:

* Обеспечивать без дополнительной оплаты разработку производителем Системы парсеров, в количестве не менее чем для 10 (десяти) различных типов данных, изначально не поддерживаемых в стандартной поставке Системы.

## Общие требования к компании разработчику

* Разработчик должен обладать экосистемой продуктов, решений и сервисов по кибербезопасности, которые обеспечивают безопасность бизнеса, критически важной инфраструктуры, государственных органов и рядовых пользователей
* Эффективность экосистемы продуктов, решений и сервисов разработчика должна иметь подтверждённую исследованием защиту и детектирование угроз на всех этапах развития атаки согласно классификации MITRE
* Экосистема продуктов, решений и сервисов разработчика должны включать решения по обеспечению детектирования и защиты от массовых угроз на конечных точках
* Продукты и решения разработчика должны обладать разнообразными международными наградами и иметь многолетние лидирующие позиции согласно независимым тестированиям на уровень качества детектирования и защиты
* Разработчик должен иметь глобальные центры экспертизы по исследованию и анализу угроз, такие как:
  + Глобальный центр по изучению вредоносного ПО и созданию способов защиты от него
  + Глобальный центр исследований и анализу угроз, выявляющий APT-угрозы
  + Глобальный центр по расследованию инцидентов и оказания помощи в реагировании на них
  + Глобальный центр по исследованию, выявлению и расследованию атак на промышленные объекты
* Разработчик должен быть участником глобальных программ обмена данными об уязвимостях, такими как Microsoft Active Protection Program, CVE или аналогичными
* Разработчик должен иметь в портфолио собственные обучающие курсы по цифровой криминалистике, анализу и обратной разработке вредоносного ПО, а также реагированию на инциденты
* Разработчик должен иметь отмеченную признанием мировых аналитических агентств лидирующую глобальную экспертизу в области Threat Intelligence, которая должна быть глубоко интегрирована в собственную экосистему работающих на её основе продуктов, решений и сервисов