ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на закупку лицензий Системы управления информации о безопасности для информационных систем
Единого Общереспубликанского Процессингового Центра

на _____ листах

действует с «____»_____ 2022 года

Ташкент 2022 г.

СОДЕРЖАНИЕ

Цели применения Системы

Основные цели применения Системы:

1. повышение общего уровня защищенности корпоративной информационной инфраструктуры;
2. консолидация и хранение журналов событий от различных источников — сетевых устройств, приложений, журналов ОС, средств защиты;
3. автоматизация процесса обнаружения инцидентов с документированием в собственном журнале, а также своевременное информирование о событиях;
4. помощь при проведении расследований произошедших инцидентов.

Требования к Системе

Требования к системе:

- Система должна обеспечивать централизованное управление всеми её компонентами и функционалом через единый веб-интерфейс;
- Система не должна иметь лицензионных ограничений по количеству пользователей, работающих с системой;
- Система не должна иметь лицензионных ограничений по количеству источников данных журналов событий;
- Система должна иметь функционал обнаружения аномальной активности пользователей (User Behavior Analytics). Допускается реализация функционала после установки в Систему бесплатного приложения;
- Система должна иметь встроенный функционал автоматической классификации определенных активов в сети;
- Система должна позволять регистрировать активы в ручном режиме;
- Система должна иметь возможность расширения своего функционала за счёт установки дополнительных приложений через магазин приложений производителя;
- Система должна иметь встроенную репутационную базу, которая обновляется производителем;
- Система должна иметь встроенный функционал обнаружения аномальной активности пользователей (User Behavior Analytics);
- Система должна поддерживать возможность разделения инструментальных панелей через пользовательский интерфейс;
- Система должна предоставлять открытый API для доступа к информации, находящейся в базе данных системы;
- Система должна иметь возможность шифровать коммуникации между компонентами;
- Система должна интегрироваться с системами сторонних производителей (LDAP, AD) для обеспечения аутентификации пользователей;

- Система должна предоставлять возможность управления, создания аналитических отчетов и правил через веб-интерфейс пользователя;
- Система должна гарантировать работу отдельных компонентов системы, при выходе из строя любой части системы. (Например, центральная консоль выходит из строя, но сборщики событий продолжают функционировать);
- Система должна иметь автоматический процесс резервного копирования конфигурации (Backup) и возможность восстановления (Recovery) конфигурации из графического интерфейса пользователя;
- Система должна иметь встроенный процесс анализа своего состояния и оповещать пользователя при возникновении проблем;
- Система должна поддерживать режимы внедрения как ПО;
- Система должна интегрироваться с другими системами обеспечения безопасности и расследования инцидентов;
- Система должна легко масштабироваться и расширять функционал (при добавлении новых устройств, офисов, приложений в сети заказчика) для соответствия требованиям бизнеса;
- Система должна поддерживать разнесенные базы данных для хранения информации о событиях, при этом вся информация должна быть доступна через единый интерфейс пользователя;
- Система должна работать при кратковременных пиках нагрузки, превышающих расчетные нагрузки для данной системы;
- Система должна обеспечивать целостность собранной информации;
- Система должна предоставлять доступ к ОС устройства. Например, возможность запустить TCP DUMP для проверки состояния системы;
- Система должна поддерживать разнесенную модель для корреляции со всех коллекторов. (Например, для 25 неудачных попыток аутентификации, когда 25 событий приходят не на 1 коллектор, а на несколько.);
- Система должна поддерживать расширенную кастомизацию для событий и полей. Пользователь должен иметь возможность присваивать событиям любые имена;
- Система должна предоставлять возможность изменения поведения автоматического тегирования событий по важности согласно пожеланиям пользователя;
- Система должна предоставлять прозрачное получение, агрегирование, сортирование, фильтрацию и аналитику данных по всем разнесенным компонентам системы;
- Система должна иметь систему сбора журналов событий и их архивации, которая поддерживает как кратковременное хранение (online), так и долгосрочное (offline) хранение журналов событий;
- Система должна поддерживать хранение журналов событий на внешних хранилищах;
- Система должна поддерживать стандартные методы сбора журналов событий (например, syslog, WMI, JDBC и пр.);
- Система должна поддерживать безагентный сбор журналов событий везде, где это возможно;
- Система должна иметь возможность распределять хранение журналов событий и их обработку по всей архитектуре системы;

- Система должна обеспечивать сбор, запись и хранение информации о событиях безопасности в течение не менее 12 месяцев;
- Система должна иметь возможность архивации журналов событий старше 4-х месяцев. При этом должен быть обеспечен доступ ко всей информации при необходимости поиска данных или дальнейших расследований;
- Система должна нормализовать стандартные поля событий (имена пользователей, IP адреса, имена хостов, устройства-источники событий) с различных устройств мультивендорной сети. Нормализация должна проводиться без дополнительной настройки («out of the box»);
- Система должна предоставлять стандартную категоризацию событий без предварительной дополнительной настройки;
- Система должна иметь возможность хранить информацию о событиях, как в исходном виде, так и в нормализованном виде для использования в дальнейших расследованиях;
- Система должна иметь возможность обрабатывать и нормализировать данные из полей, которые не поддерживаются изначально и не предоставляются с настройками «out of the box»;
- Система должна обеспечивать анализ событий в режиме реального времени;
- Система должна обеспечивать анализ событий на протяжении определенного периода времени;
- Система должна предоставлять возможность собирать и анализировать события по предустановленным пользователем фильтрам;
- Система должна предоставлять возможность получения дополнительной информации о событиях при необходимости (функция «drill down»);
- Система должна обеспечивать фильтрацию, а также показывать через интерфейс пользователя события в режиме реального времени, где пользователь может сразу же применять политики и фильтры;
- Система должна предоставлять отчетность по всем событиям, отчетность должна быть доступа через веб-интерфейс для пользователей решения;
- Система должна давать возможность самостоятельной настройки отчетности и создания собственных отчетов пользователем;
- Система должна иметь возможность планирования генерации отчетов в определенный период времени;
- Система должна предоставлять примеры сгенерированных отчетов для более простого использования и генерации новых отчетов пользователем, а также мастер создания отчетов;
- Система должна предоставлять удобный интерфейс для быстрой визуализации все информации о сети и безопасности;
- Система должна предоставлять отчеты за определенный период времени по различным сегментам и системам в сети;
- Система должна предоставлять возможность автоматического распределения отчетов;
- Система должна обеспечивать корреляцию информации с различных источников, которые никак не взаимодействую между собой;
- Система должна обеспечивать оповещения на основе обнаруженных аномалий и поведенческого анализа и изменений;

- Система должна обеспечивать оповещения по предустановленным политикам (например, при обнаружении трафика, который запрещен.);
- Система должна обеспечивать оповещения исходя из сегмента сети, а также типа трафика;
- Система должна поддерживать приоритезацию оповещений в зависимости от требований пользователя, а также критичности активов;
- Система должна обеспечивать возможность создания собственных настраиваемых оповещений;
- Система должна предоставлять мастер настройки оповещений для упрощения процесса их создания, а также улучшения точности результатов и уменьшения количества ложных срабатываний;
- Система должна предоставлять возможность создания оповещений при превышении/нарушении норм работы систем и их использования;
- Система должна иметь возможность ограничивать число одинаковых оповещений на единицу времени;
- Система должна использовать графический интерфейс пользователя для настройки и демонстрации оповещений;
- Система должна иметь возможность применять активное воздействие и реакцию на оповещения. Например, отправлять письмо по почте;
- Система должна поддерживать интеграцию (на уровне оповещений) с другими системами безопасности и оповещения, которые функционируют в сети;
- Система должна предупреждать, администратора, если перестали поступать логи с устройства в сети, которое мониторится (например, нет логов от сервера в течении 10-ти минут);
- Система должна обеспечивать встроенный функционал определения всех устройств и их инвентаризации по классам систем (например, почтовые сервера, сервера баз данных и пр.) для минимизации количества ложных срабатываний из-за недостатка информации о системах;
- Система должна обеспечивать корреляцию по определенным последовательностям событий. Например, сервис остановился и не возобновляется на протяжении 10 минут;
- Система должна поддерживать корреляцию на основе дополнительных данных. Например, на основе журналов событий с firewall, которые содержат поля с объемом переданных данных (например, когда источник пересылает более 1GB данных, через один порт серверу, за 1 час).
- Система должна поддерживать обработку поступающих событий со скоростью не менее 1100 событий в секунду.
- Система должны поддерживать обработку сетевых потоков со скоростью не менее 15000 потоков в минуту.
- Система должна уметь проводить поведенческий анализ трафика и сообщать об изменениях согласно заданных порогов изменения.
- Система должна детектировать DoS и DDoS атаки.
- Система должна детектировать и отображать трафик, относящийся к угрозам. Выдавать информацию по типам угроз в сети.
- Система должна поддерживать разделение трафика согласно логическому дизайну сети. (т.е., Subnet/CIDR).

- Система должна предоставлять информацию в нескольких интервалах времени (за неделю, день и час).
- Система должна определять происхождение и назначение потоков трафика в сети, в том числе и по географическим регионам в режиме реального времени.
- Система должна разделять и создавать независимые профайлы для локального трафика и трафика идущего/приходящего в/из интернет.
- Система должна позволять создавать пользовательские профайлы используя для выборки любые параметры потока трафика.
- Система должна поддерживать представление трафика на основе IP адреса, группы IP адресов, источник/место назначения IP пар и т.д.
- Система должна иметь возможность контекстно связывать активность приложения в сети с событием безопасности на подконтрольном устройстве.
- Система в реальном времени должна контекстно связывать выявленные события безопасности со знаниями об активах в сети.
- Система должна обеспечивать представление информации событий в реальном времени (как в оригинальном/сыром виде, так и в обработанном формате).
- Система должна обеспечивать способность отсылать уведомление о тревогах определенными методами (т.е., SNMP trap, e-mail, и т.д.).

Требования к совместимости Системы

6. Все компоненты системы должны быть частью единой системы управления инцидентами безопасности;
7. Система должна обеспечивать централизованное управление всеми компонентами и функционалом через единый веб-интерфейс;
8. Развертывание всех модулей системы должно обеспечиваться с единого образа ПО, а необходимый функционал активироваться лицензией без необходимости установки дополнительного ПО;
9. Система должна поддерживать расширения своего функционала за счет добавления дополнительных модулей на лицензий :
- Система должна предоставлять возможность внедрения функционала анализа сетевого трафика на уровне приложений (Layer 7 OSI);
- Система должна предоставлять возможность внедрения функционала анализа сетевого на трафике на уровне приложений в виртуализованных инфраструктуре на базе VMware;
10. Вся информация по событиям, по сетевым потокам и об инцидентах должна собираться, обрабатываться и храниться в единой базе данных без необходимости запуска и использования сторонних приложений, баз данных, дополнительных интерфейсов, скриптов или других виртуальных устройств;
11. Система должна гарантировать актуальность данных, собираемых и обрабатываемых в единой базе данных - обеспечивать обработку и корреляцию данных из журналов событий (logs) и потоков (flows) с задержкой не более 1 секунды после получения данных системой от источника событий или потоков;
12. Все компоненты системы должны иметь единую базу данных для хранения и обработки информации.

Требования к Технической поддержке Системы

1. Техническая поддержка по Системе должна предоставляться в срок не менее 1 года с момента поставки.
2. Техническая поддержка должна включать возможность получения новых версии и обновлений Системы в течение срока действия.
3. Техническая поддержка должна включать возможность заведения обращений производителю Системы для устранения ошибок функционирования Системы, а также для восстановления Системы после критических ошибок.

Требования к Исполнителю

4. Исполнитель должен соответствовать требованиям, устанавливаемым в соответствии с законодательством Республики Узбекистан к организациям, осуществляющим поставки товаров, выполнение работ, оказание услуг, являющихся лицензируемыми видами деятельности, что подтверждается наличием соответствующей(их) лицензии(ий) у Исполнителя.
5. Исполнитель должен быть Авторизованным партнером производителя Системы в Республике Узбекистан на дату своего предложения.
6. Исполнитель должен обладать практическим опытом выполнения работ по обеспечению информационной безопасности не менее 1 года, а также наличие не менее двух сертифицированных производителем Системы сотрудников, граждан Республики Узбекистан.