1. Введение

Полное наименование работ: Создание Системы мониторинга событий информационной безопасности.

Краткое наименование системы: SIEM

Заказчик: АКБ «Hamkorbank» (далее – Банк). Адрес: Республика Узбекистан, 710011, город Андижан, проспект Бобура, дом 85.

Сроки выполнения работ: не более x дней с даты подписания Договора.

2. Цели и задачи

- Целью SIEM-системы является обеспечение комплексного мониторинга безопасности, обнаружения и предотвращения инцидентов, анализа угроз и создания отчетов для поддержки принятия решений.
- Основные задачи системы включают сбор, агрегацию, корреляцию и анализ различных типов данных, включая логи событий, потоки сетевого трафика, события системного мониторинга и данные угроз безопасности.
- SIEM предназначена для автоматизация централизованного сбора, корреляции и анализа событий информационной безопасности в АКБ «Hamkorbank».

3. Требования к функциональности

- Сбор данных:
  - Интеграция с различными источниками данных, такими как серверы, сетевые устройства, приложения, базы данных, брендмауэры, системы обнаружения вторжений (IDS) и системы управления угрозами (Threat Intelligence).
  - Поддержка различных протоколов и форматов данных, включая Syslog, SNMP, CEF (Common Event Format), JSON и XML.
  - Способность обрабатывать большие объемы данных и обеспечивать высокую пропускную способность.
- Корреляция и анализ:
  - Автоматическая корреляция и анализ данных для обнаружения связанных событий и аномалий.
  - Использование правил, сценариев (use cases) и алгоритмов машинного обучения для выявления подозрительного поведения и угроз безопасности.
  - Возможность создания пользовательских правил и сценариев для адаптации системы к особенностям организации.
- Управление инцидентами:
  - Регистрация, классификация и приоритизация инцидентов с учетом их серьезности и влияния на бизнес.
  - Автоматизация обработки инцидентов, включая автоматическое уведомление, анкетирование и назначение ответственных лиц.
  - Возможность создания и отслеживания рабочих задач для решения инцидентов.

- Отчетность и аналитика:
    - Создание гибких отчетов, дашбордов и графиков для визуализации статистики, трендов и метрик безопасности.
    - Поддержка стандартных шаблонов отчетов, таких как PCI DSS (Payment Card Industry Data Security Standard) и HIPAA (Health Insurance Portability and Accountability Act).
    - Возможность настраивать и экспортировать отчеты в различных форматах, включая PDF, CSV и HTML.
    - Возможность использования настраиваемых запросов в базу событий SIEM для построения графиков и отчетов.
    - Возможность редактирования существующих или создания новых нормализаторов событий.

4. Требования к производительности

- Пропускная способность:
    - Обеспечение высокой скорости сбора, обработки и анализа данных для обеспечения реального времени или близкого к нему мониторинга безопасности.
    - Масштабируемость системы чтобы справиться с ростом объема данных и количества подключенных источников.
- Хранение данных:
    - Возможность хранить данные в течение длительного времени в целях анализа и аудита.
    - Гибкость в выборе метода хранения данных, включая использование реляционных баз данных, NoSQL-решений или облачных хранилищ.

5. Требования к безопасности

- Аутентификация и авторизация:
    - Использование сильных механизмов аутентификации и авторизации для защиты доступа к системе и ее функциональным компонентам.
    - Поддержка интеграции с существующей инфраструктурой управления идентификацией, такой как Active Directory или LDAP (Lightweight Directory Access Protocol).
- Шифрование данных:
    - Шифрование данных в покое и в движении для защиты конфиденциальности и целостности информации.
    - Поддержка протоколов шифрования, таких как SSL/TLS (Secure Sockets Layer/Transport Layer Security).
- Мониторинг безопасности:
    - Возможность мониторинга и обнаружения попыток несанкционированного доступа, атак и других угроз безопасности системы SIEM.
    - Интеграция с системами обнаружения вторжений (IDS) и системами предотвращения вторжений (IPS) для реагирования на активности злоумышленников.
- Аудит и трассировка:
    - Регистрация и аудит действий пользователей и системных событий для обеспечения возможности ретроспективного анализа и расследования инцидентов.

- Сохранение аудитных журналов в защищенном хранилище с ограниченным доступом.

6. Интеграция и масштабирование

- Интеграция с существующей инфраструктурой:
  - Поддержка протоколов и стандартов интеграции, таких как RESTful API (Application Programming Interface) и SNMP (Simple Network Management Protocol).
  - Возможность интеграции с сетевыми устройствами, системами мониторинга угроз, системами аутентификации и другими системами безопасности.
- Масштабируемость:
  - Горизонтальное и вертикальное масштабирование системы для обработки растущего объема данных и повышения производительности.
  - Возможность добавления новых узлов и компонентов без прерывания работы системы.

7. Требования к поддержке и обслуживанию

- Обновления и поддержка:
  - Предоставление регулярных обновлений программного обеспечения, исправлений ошибок и патчей безопасности.
  - Механизмы автоматического обновления и проверки наличия обновлений.
  - Техническая поддержка и доступ к базе знаний для решения проблем и запросов пользователей.
  - Резервное копирование и восстановление:
  - Возможность создания резервных копий данных системы и конфигурации для обеспечения возможности восстановления в случае сбоя или потери данных.
  - Тестирование процесса восстановления и регулярное создание резервных копий.
- Мониторинг и оповещение:
  - Возможность мониторинга состояния системы, производительности, доступности и уровня сервиса.
  - Оповещение администраторов и ответственных лиц в случае обнаружения проблем и событий, требующих внимания.

8. Инфраструктура и требования к развертыванию

- Аппаратные требования:
  - Определение необходимых аппаратных ресурсов, таких как серверы, хранилища данных и сетевое оборудование, для развертывания системы SIEM.
  - Указание требуемых характеристик серверов, включая процессоры, оперативную память, дисковое пространство и сетевые интерфейсы.
  - Установка рекомендуемых операционных систем и конфигурация сетевых настроек.
- Программное обеспечение:

    - Установка и конфигурация операционной системы и пререквизитов, необходимых для работы системы SIEM, таких как базы данных, веб-серверы и прокси-серверы.
    - Развертывание и настройка программных модулей системы SIEM, включая центральный сервер, коллекторы данных и агенты сбора данных.
- Интеграция с существующей инфраструктурой:
    - Установка и настройка необходимых интеграций с другими системами безопасности, такими как IDS/IPS, антивирусные программы и системы аутентификации.
    - Проверка совместимости и настройка соответствующих протоколов и стандартов интеграции, таких как Syslog, SNMP и RESTful API.
    - Масштабирование и высокая доступность:
    - Разработка архитектуры, обеспечивающей возможность горизонтального и вертикального масштабирования системы SIEM для обработки растущего объема данных.
    - Настройка механизмов высокой доступности, таких как кластеризация серверов, резервирование ресурсов и механизмы отказоустойчивости.

9. Требования к документации

- Руководства пользователя:
    - Создание подробного руководства пользователя, объясняющего функциональность системы, процессы анализа и использование инструментов.
    - Инструкции по развертыванию и настройке:
    - Документация, описывающая процесс развертывания системы, настройку компонентов и интеграцию с существующей инфраструктурой.
    - Документация по поддержке и обслуживанию:
    - Создание документации, описывающей процессы поддержки, обслуживания, резервного копирования, восстановления и мониторинга системы.