РТИ

радиолокация
технологии
информация

24 августа 2018г.

www.oaorti.ru

Современные большие АСУ требуют новых подходов к системе безопасности

РТИ радиолокация технологии информация

- Рост количества оборудования и средств защиты в IT-инфраструктуре уже не позволяет администраторам ИБ ограничиваться встроенными средствами обеспечения ИБ – требуется средство консолидации всех событий ИБ в одном инструменте
- Распространение целевых атак требует новых методов обнаружения инцидентов ИБ
- Информацию о событиях и инцидентах ИБ требуется хранить и иметь возможность оперативного доступа для ее анализа – требуется система с поддержкой горизонтального масштабирования
- Большой объем поступающих данных за момент времени может быть оперативно обработан только системой с мощным корреляционным механизмом
- Своевременное выявление новых угроз информационной безопасности, целенаправленных атак и оперативное реагирование на них.

РТИ разработало СУИБиКС для поддержки работы больших АСУ

радиолокация
технологии
информация

Система управления инцидентами безопасности и корреляции событий (СУИБиКС) разработки РТИ предназначена для:

- Своевременного выявления новых угроз информационной безопасности и целенаправленных атак
- Сбора и накопления большого количества событий информационной безопасности с разнородных источников
- Глубокого анализа обстановки в ИТ-инфраструктуре
- Выявления аномального поведения пользователей за счет машинного обучения Системы и принятия решения о реагировании на возникающие угрозы информационной безопасности

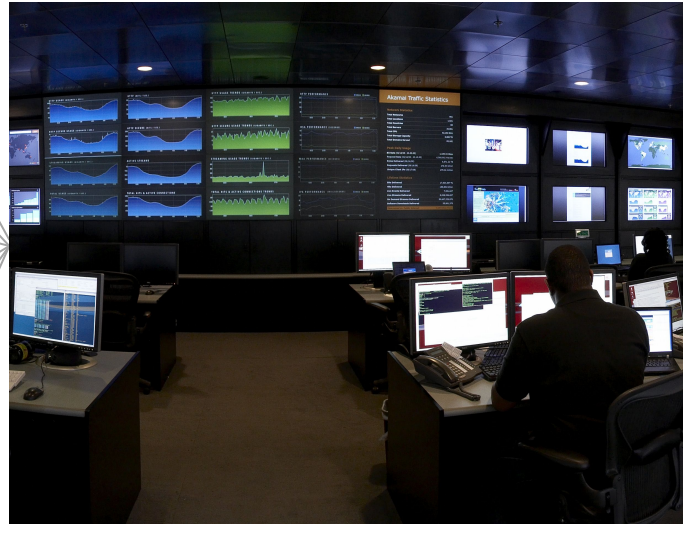
СУИБ и КС - единая система, позволяющая расследовать инциденты и оперативно реагировать на угрозы ИБ

РТИ радиолокация технологии информация

Система управления инцидентами безопасности и корреляции событий (SIEM) – распределенная высоконагруженная система с поддержкой кластеризации, горизонтального масштабирования и анализа данных, интегрированная с разнородными средствами защиты информации.

Система управления инцидентами безопасности и корреляции событий

- АРМ и сервера
- Сетевое оборудование
- АПМДЗ и антивирусы
- ИПТК Капитан
- ПО обнаружения вторжений
- Датчики целевых атак



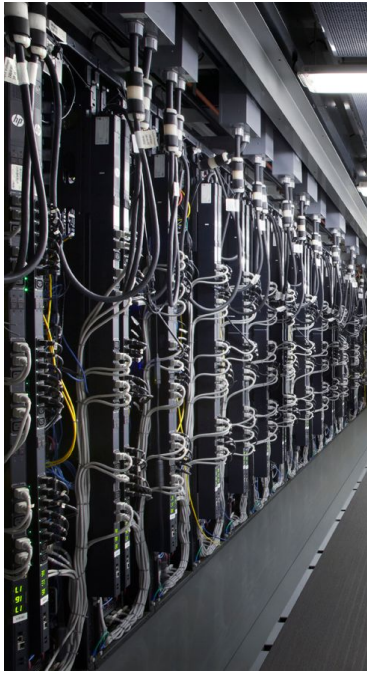
- Мониторинг событий ИБ
- Обнаружение и расследование инцидентов ИБ
- Защита от новых угроз ИБ и целевых атак
- Анализ больших данных ИБ

Система управления инцидентами безопасности и корреляции событий (SIEM) с применением технологий искусственного интеллекта

SIEM-система и технологии искусственного интеллекта

радиолокация
технологии
информация

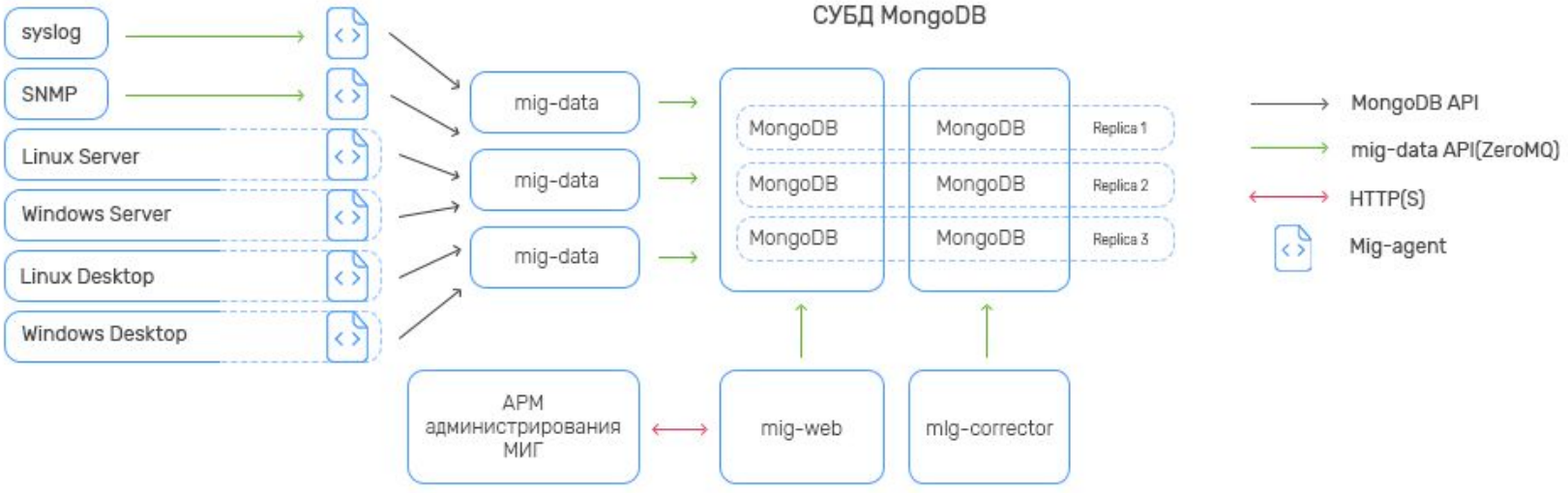
В контексте Системы управления инцидентами безопасности и корреляции событий искусственный интеллект (ИИ) – это ПО, способное интерпретировать события безопасности, распознавать происходящие в ней аномалии и самостоятельно реагировать на возникающие новые угрозы информационной безопасности и целенаправленные атаки.



ИИ не может заменить аналитиков (экспертов) по информационной безопасности, но его преимущества неоспоримы:

- ИИ особенно хорошо справляется с распознаванием **закономерностей и аномалий**
- ИИ функционирует с использованием **машинного обучения**, которое позволяет SIEM-системе анализировать огромные объемы данных и делать соответствующие выводы для выявления аномалий поведения пользователей
- ИИ **совершенствуется** по мере роста объема получаемых данных. При накоплении достаточно больших срезов данных Система способна обнаруживать очень ранние признаки появления новых угроз информационной безопасности и целенаправленных атак
- SIEM-система **всегда обучается и никогда не забывает**, поэтому чем больше она собирает информации, тем становится более интеллектуальной

Архитектура SIEM



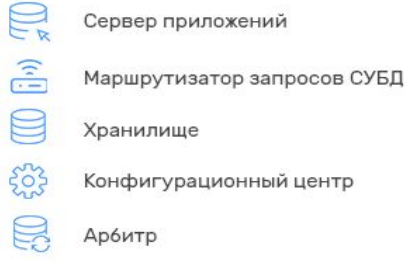
Ключевые компоненты:

- **Сервис сбора данных** отвечает за прием данных от Агентов, их регистрацию, аутентификацию, контроль целостности передаваемых данных и категоризацию событий ИБ
- **Сервис анализа данных** обеспечивает вычисление количественных метрик событий ИБ, осуществляет обнаружение инцидентов ИБ и аномалий поведения пользователей. Корреляция событий ИБ производится двумя независимыми механизмами. Первый механизм – rule-based корреляция в режиме реального времени. Второй - статистический детектор аномалий
- **Веб-интерфейс** – основной инструмент для администратора безопасности. Обеспечиваются функции просмотра и поиска событий ИБ, инцидентов, управление расследованием инцидентов, настройка правил корреляции, построение отчетов

Поддерживаются следующие типы источников событий ИБ:

- Текстовый файл;
- Журнал событий Windows;
- Syslog;
- SNMP;
- СУБД SQL;
- Netflow;
- Мониторинг файлов на сетевых ресурсов

Обеспечение надежности и горизонтального масштабирования SIEM



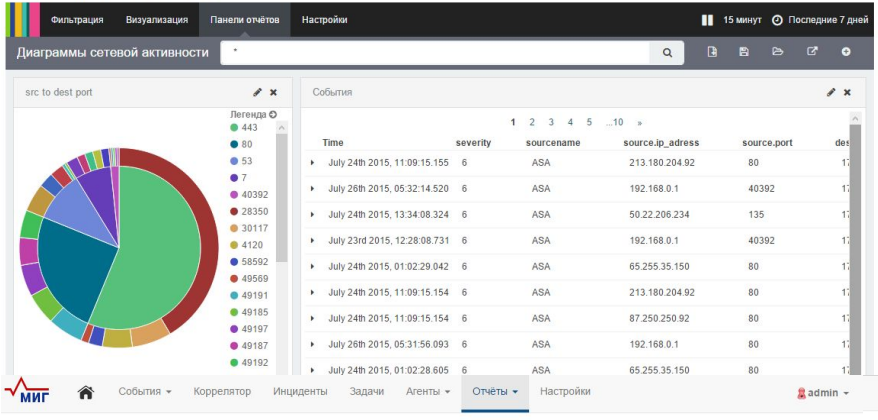
- SIEM обладает архитектурой, устойчивой к потере до 60% узлов, отвечающих за сбор и хранение событий и инцидентов ИБ.
- На схеме приведена архитектура SIEM с тройным резервированием и двукратным масштабированием хранилища данных.

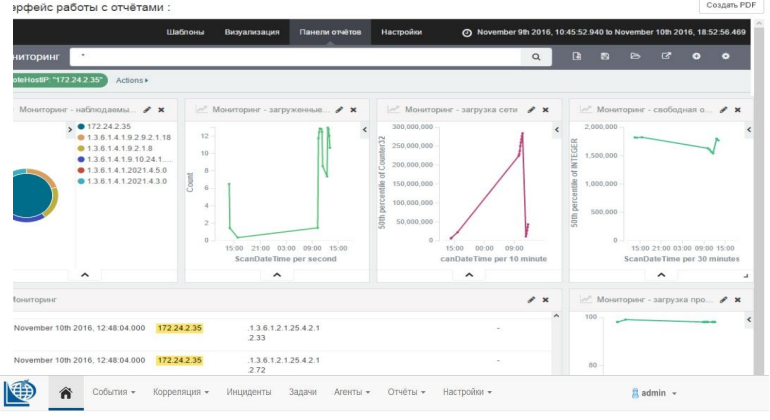
- Тройное резервирование информации о событиях и инцидентах ИБ позволяет не только сохранить данные, но и увеличить производительность анализа инцидентов ИБ до трех раз

WEB интерфейс

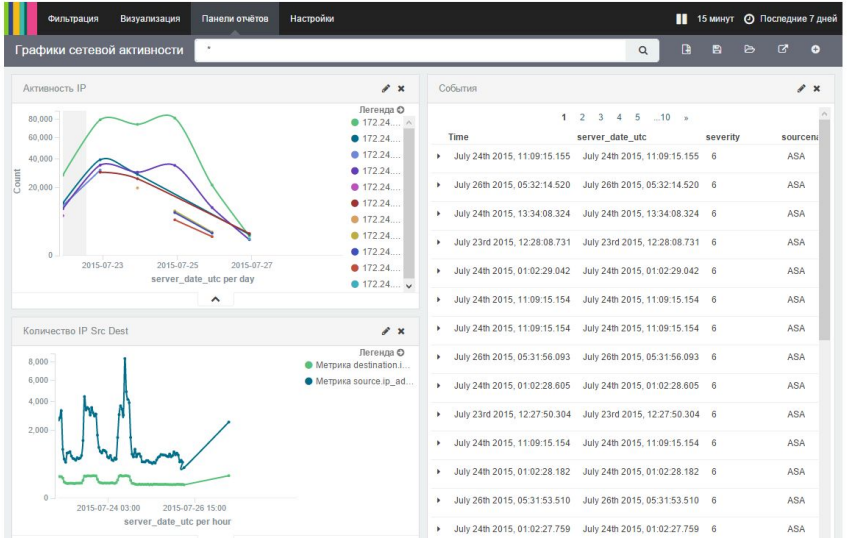
радиолокация технологии информация

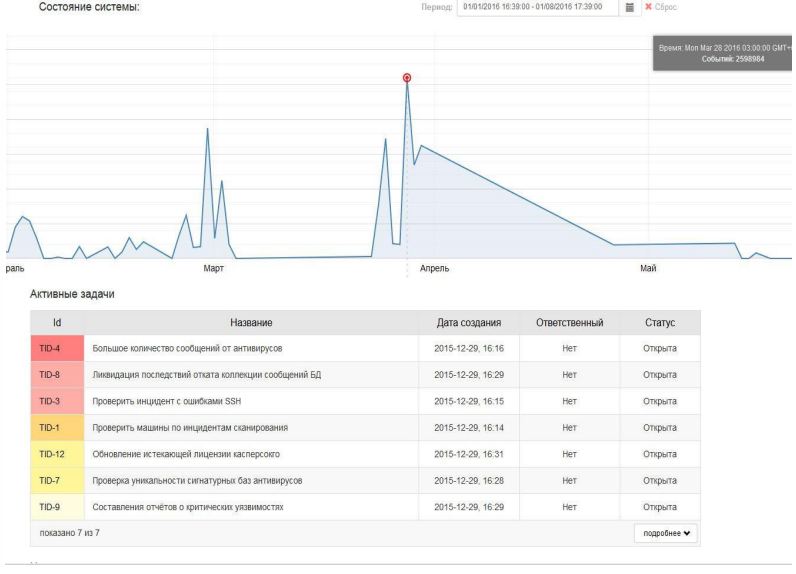
Интерфейс работы с отчётами :





Интерфейс работы с отчётами :





Система управления инцидентами безопасности и корреляции событий (SIEM) с применением технологий искусственного интеллекта

РТИ радиолокация технологии информация

Благодарим Вас за внимание

Москва, ул. 8 Марта, д.10 стр.1
Тел.: +7 (495) 788-00-07
Факс: +7 (495) 614-22-62

www.aorti.ru