Практика использования систем управления информацией о безопасности и событиями безопасности

Сергей Шерстюк
АйТи Таск

Что творится в инфраструктуре?

Большое количество сетевых устройств, приложений

Распределенная инфраструктура

Непонятный исходный формат событий

Кто дал полный доступ к базе данных для нового сотрудника

Увидеть инцидент в логах нереально. Необходима масса факторов

Не будем смотреть логи – об инцидентах узнаем из газет

Реагировать на каждый чих систем безопасности – неправильно!

Стирание, переполнение журнала событий

А «насколько плох вот этот алерт?» - нет данных о критичности и влияния на процессы

Применяемые методы позволяют оператору понимать «о чем это событие»

Средства workflow позволяют контролировать работу над инцидентами, а не оставлять их забытыми без внимания

SIEM не отразит все атаки, но поможет упорядочить хаос, расследовать уже произошедшие инциденты и не допускать новых

Инвентаризация и комплайнс

Сохранять все события так как это может сказаться на расследовании инцидентов, собрать доказательную базу

Оператор не должен просматривать все события, а только важные инциденты (уже готовые выводы)

SIEM
и регуляторы

Requirement 10: Track and monitor all access to network resources and cardholder data Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

Article 30 EU GDPR
"Records of processing activities"

«1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility...»

Примеры реализации

Фрод и мошенничество

Обнаружение НСД (вход под учетной записью уволенного сотрудника)

Изменение конфигураций «не админами»

Повышение привилегий

Выявление несанкционированных сервисов

Аномальная активность пользователя (массовое удаление/копирование)

Контроль выполняемых команд на серверах и сетевом оборудовании

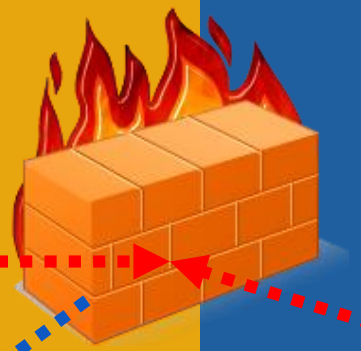
Выполнение требований законодательства и регуляторов

Аудит изменений конфигураций (сетевых устройств, приложений, ОС)


Сетевые инциденты
Доступ к критичным ресурсам в нерабочее время
Многочисленные неуспешные попытки авторизации на точке доступа
Доступ извне к внутренним критичным ресурсам
Контроль межзонных соединений (DMZ to Internet, Test zone – Production
Многочисленные попытки соединения с множеством хостов
Обнаружение траффика на нестандартных портах
Очистка журналов событий на оборудовании
Изменение конфигурации сетевого оборудования

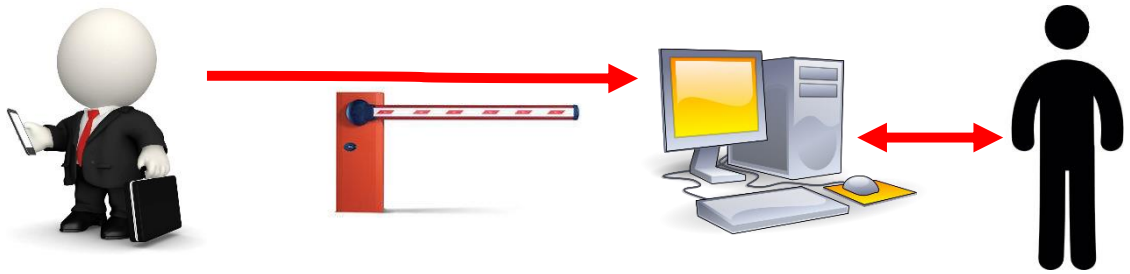
LAN

Internet



Контроль доступа на разных уровнях

Есть авторизация на АРМ...



Microsoft Active Directory

Rusiem
ВСЁ ПОД КОНТРОЛЕМ

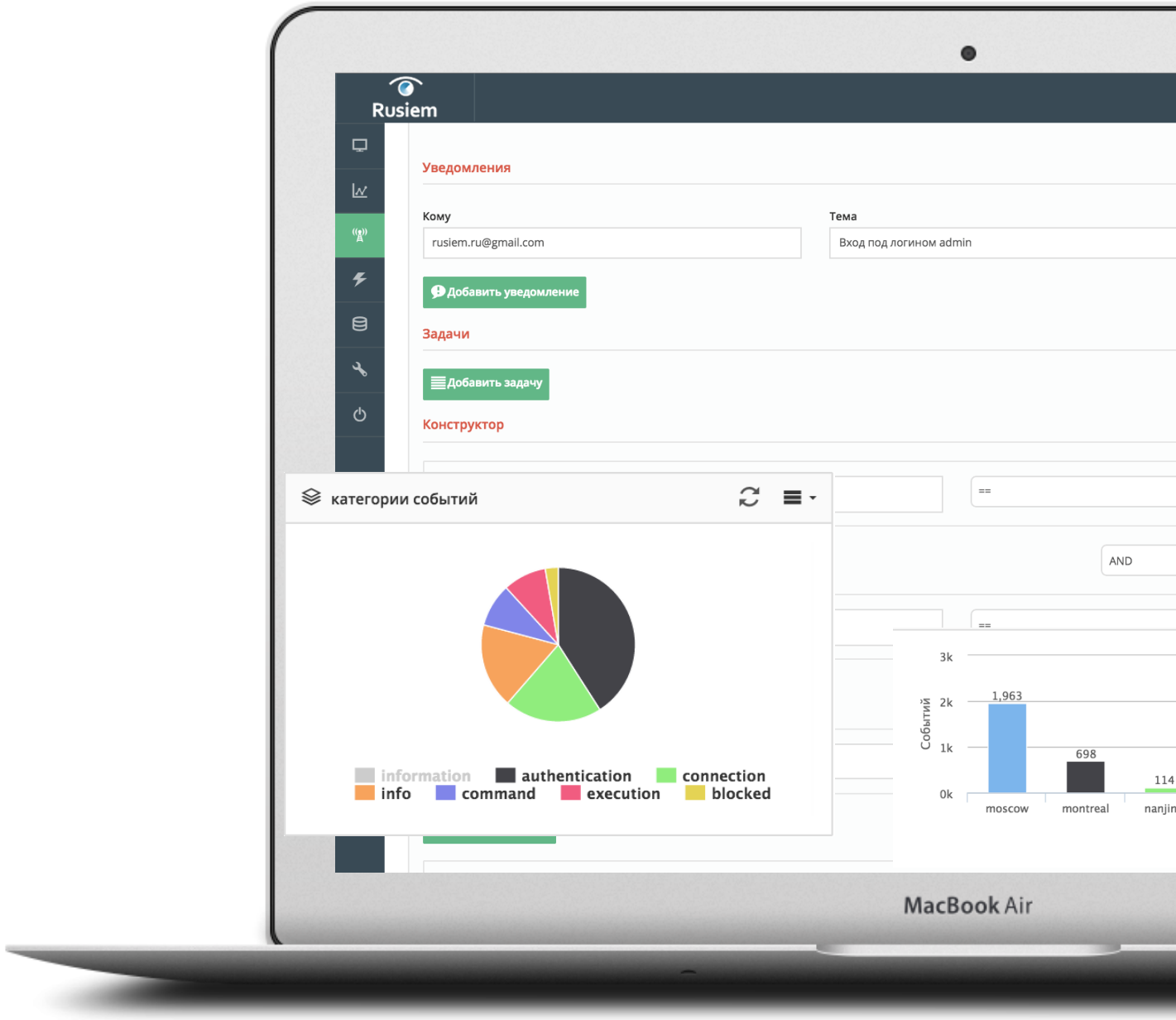
...не зафиксирован проход через СКУД.

ИНЦИДЕНТ?

Rusiem

ВСЁ ПОД КОНТРОЛЕМ

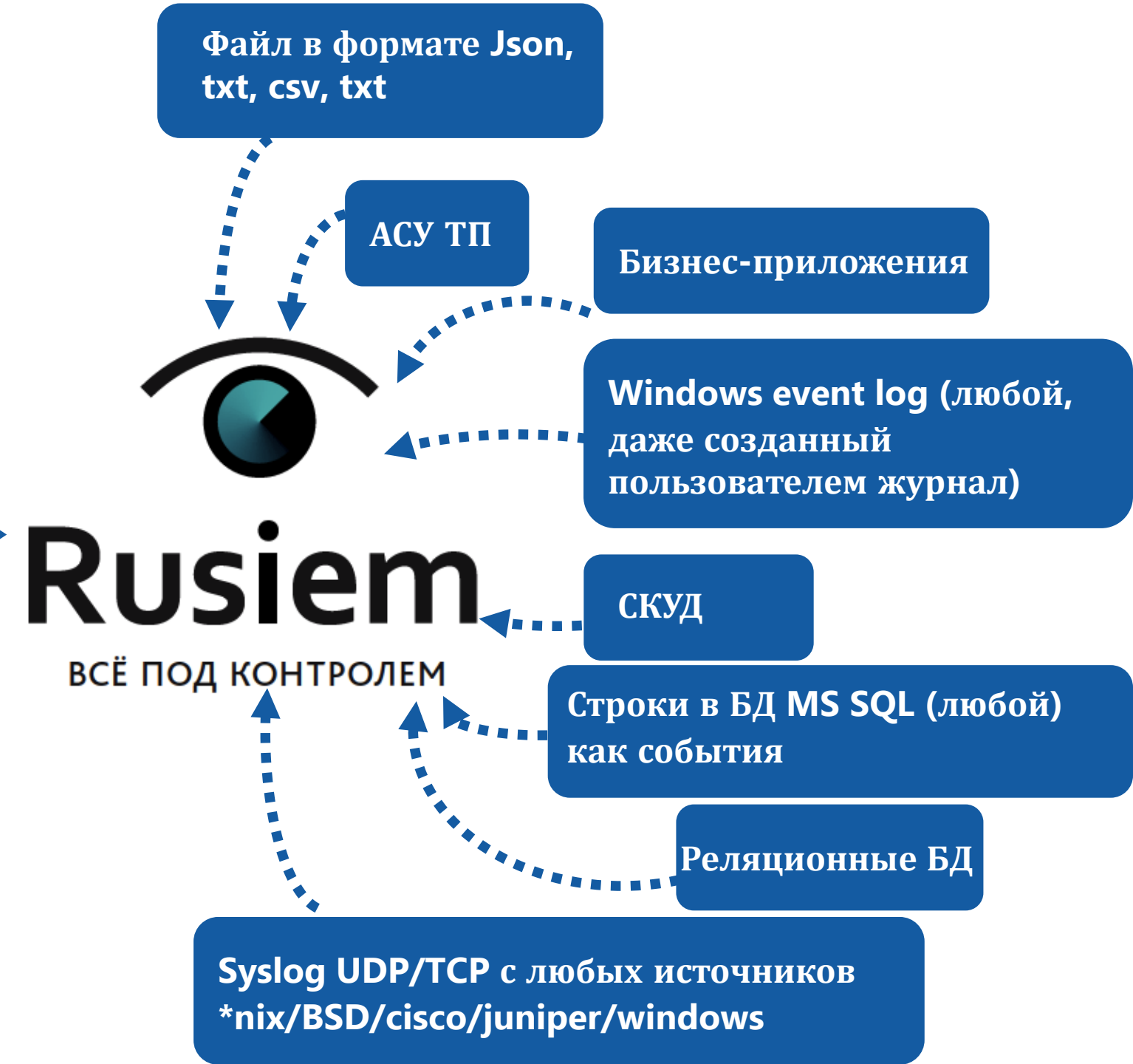
- Собственная разработка
- Приведенная к общему формату объектная нормализация
- Встроенная управляемая и редактируемая корреляция
- Высокая производительность (Свыше 90000 событий на одну ноду).
- Нет ограничений по количеству событий и источникам
- Сохранение исходных RAW-событий
- Нет ограничений по размеру архивного хранилища
- Коннекторы от производителя
- Наличие собственных модульных агентов.
- Разделение нагрузки на несколько серверов или виртуальных машин.
- Легкая вертикальная масштабируемость.



Real-time и историческая корреляция с возможностью настройки правил пользователем

Отсутствие необходимости приобретения дополнительного ПО

Собственный Workflow для инцидент-менеджмента



Испытайте RuSIEM в вашей инфраструктуре!

- Пилоты бесплатные!
- Пилотная лицензия - 3 месяца
- Выделенный инженер
- По итогам составляется ПМИ и проводятся испытания

Rusiem

ВСЁ ПОД КОНТРОЛЕМ

Сергей Шерстюк

s.sherstyuk@it-task.ru
+7 (916) 100-77-68

it-task.ru
rusiem.com