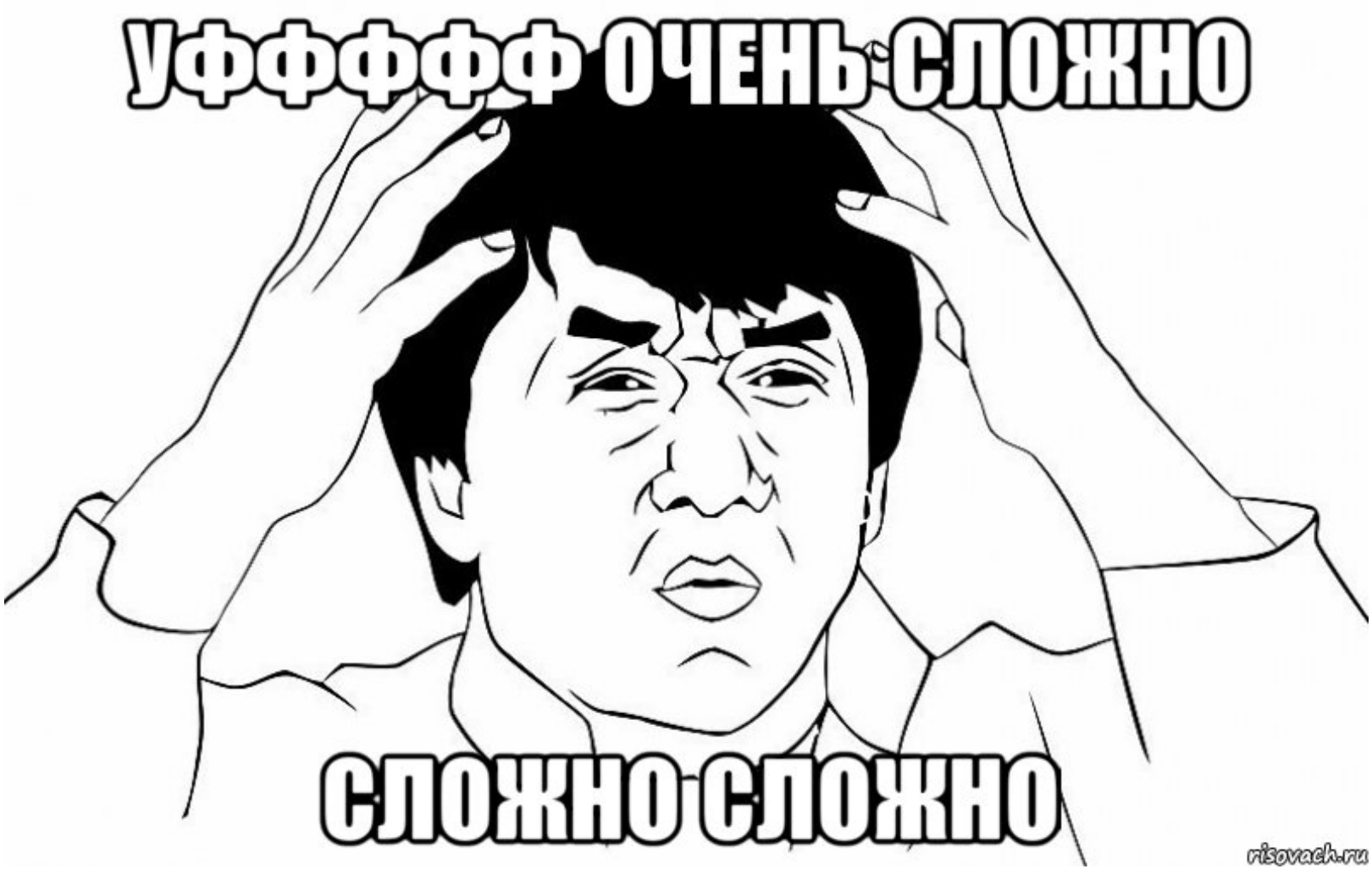
105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Практики использования SIEM. Необходимость/достаточность SIEM для SOC?

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Вы видели время и прошлые доклады?



105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Практика использования SIEM

- Антивирус
- Межсетевой экран
- СКУД
- Целевые системы
- DLP
- СЗИ от НСД
- Средства защиты виртуализации

Когда Вы проверяли статус?

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Предпосылки возникновения SIEM

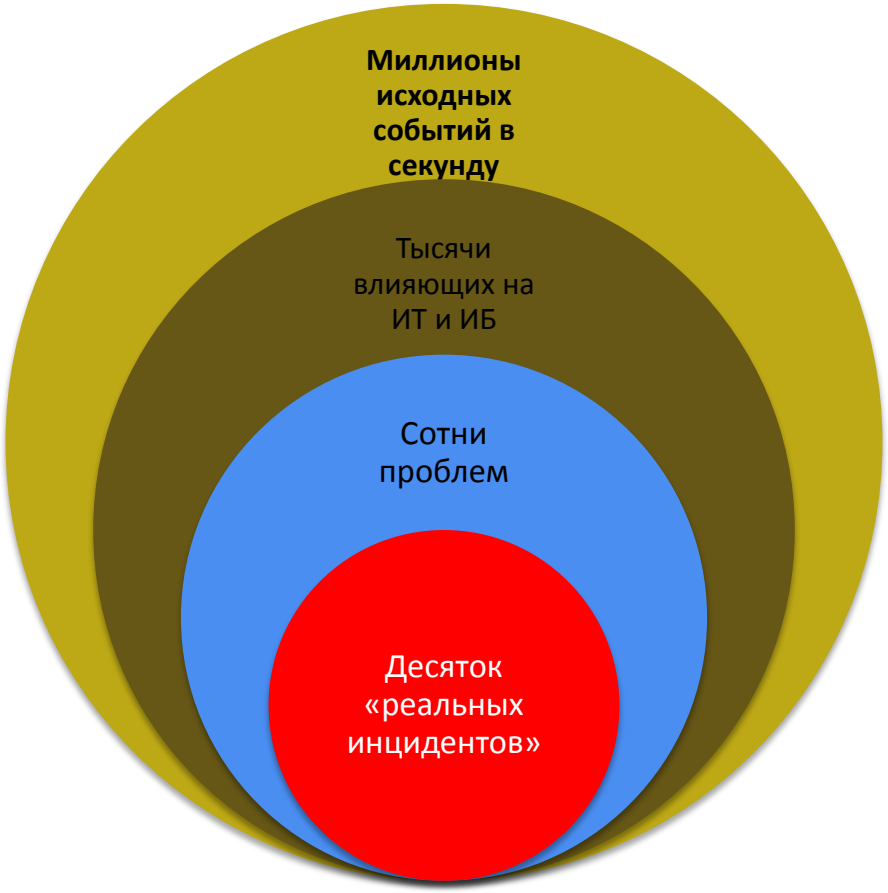
- Большое количество сетевых устройств, приложений;
- Распределенная инфраструктура;
- Непонятный исходный формат событий
- Что происходит в инфраструктуре (отказы, эпидемии, атаки, несанкционированный доступ)
- Почему и откуда блокируются учетные записи
- Кто дал полный доступ к базе данных для нового сотрудника
- Что с этой информацией делать?
- Логи нельзя удалить?

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Что я думаю о SOC'ах

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Необходимость/достаточность SIEM для SOC



- Я не верю, что все обработаете без качественное автоматизации обработки событий!
- Я не верю, что человек умеет читать логи!
- Люди ошибаются!
- 1 сотрудника достаточно для SOC
- 3 сотрудников мало для SOC
- Да поймите разницу между мониторингом и реагированием на инциденты!

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

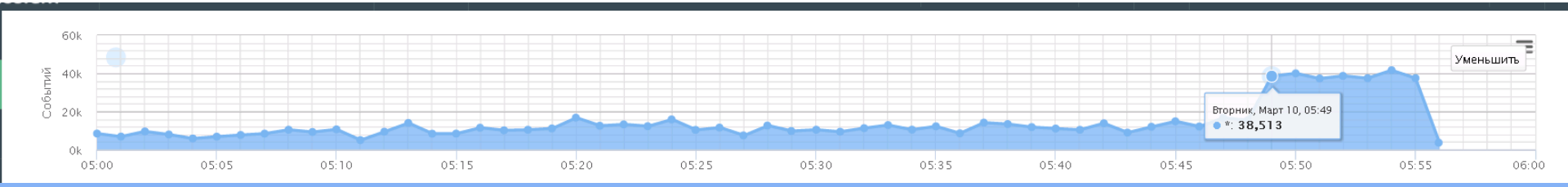
Что мы предлагаем?

Rusiem

ВСЁ ПОД КОНТРОЛЕМ

Основные преимущества:

- Собственная разработка, не зависящая от санкций и развития open-source.
- Полная поддержка русского языка
- 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!
- Real-time и историческая корреляция.
- Наличие собственных модульных агентов.
- Разделение нагрузки на несколько серверов или виртуальных машин.
- Легкая вертикальная масштабируемость.



105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Вопросы

ООО «АйТи Таск»

- **Тел./факс**: +7 (495) 972-98-26
- **Адрес:** 105082, Россия, г. Москва
  ул. Большая Почтовая 55/59с1
- **E-mail:** info@it-task.ru
- **Web:** www.It-task.ru