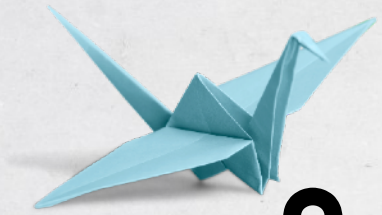
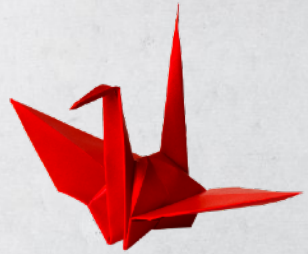


Опыт построения SOC на базе SIEM-системы RuSIEM

Даниил Вылегжанин

руководитель отдела предпродажной подготовки
компании RuSIEM



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
ИТОГИ

КОД ИБ ИТОГИ 2023

МОСКВА

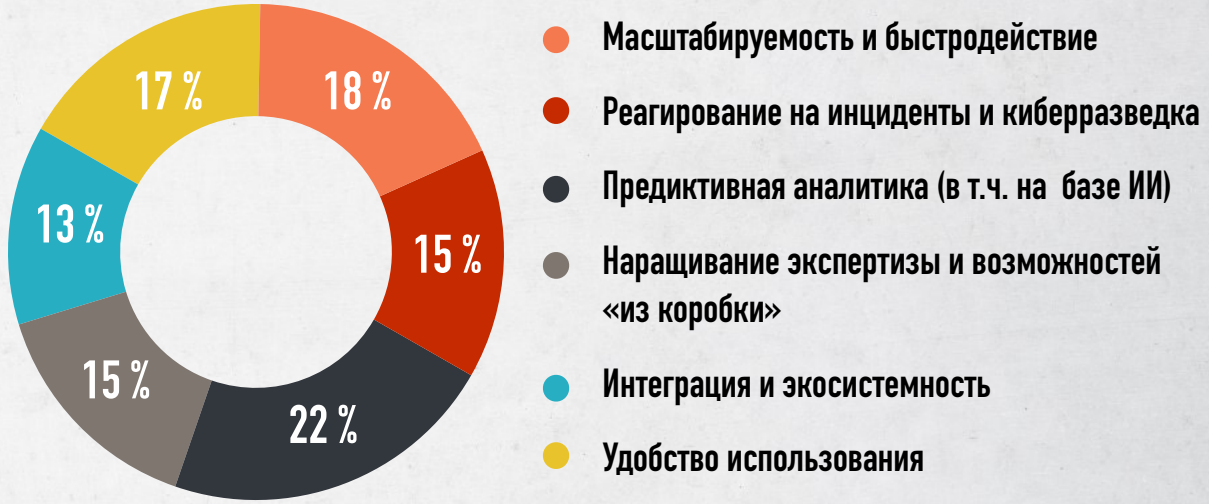
07 ДЕКАБРЯ 2023

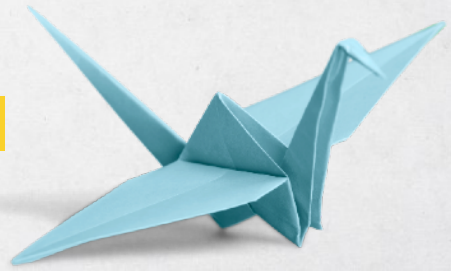
ПАЛЬМИРА БИЗНЕС КЛУБ

Аналитика по отрасли (SIEM)

- Активное развитие рынка отечественных SIEM-систем и выход на рынок новых игроков
- Успешная миграция на российские SIEM: сложностей при миграции все меньше, а решения становятся все более технологичными и зрелыми
- SIEM остаётся центральным инструментом выявления компьютерных атак, массовость и сложность которых неуклонно возрастают

Тенденции развития российских SIEM?

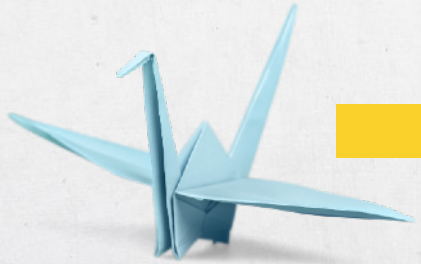




Аналитика по сегменту (SOC)

- Повышение количества запросов на создание частных SOC
- Рост доверия заказчиков к использованию услуг коммерческих SOC
- SOC на базе RuSIEM развернут для ряда крупных заказчиков совместно с партнерами:

Количество заказчиков, использующих SOC на базе RuSIEM в 2023 году выросло более, чем в 15 раз



Выводы и итоги

- Активный рост в развитии отечественных SIEM-систем
- По предварительным подсчетам рост в 2 раза относительно итогов 2022 года (в 2022 году был зафиксирован 3х – кратный рост по отношению к 2021 году)
- Технологическое развитие RuSIEM, выпуск новых модулей
- 4 мажорных релиза за 2023 год, готовим к выпуску 5-й с обновленным дизайном системы
- Усиление экспансии на международной арене (новые рынки)
- Значительный рост партнерской сети и числа заказчиков разных сфер деятельности