infotecs

Технологии обнаружения компьютерных атак

Методы обнаружения

A long time ago…

infotecs

1984

- Signature detection

Наше время

infotecs

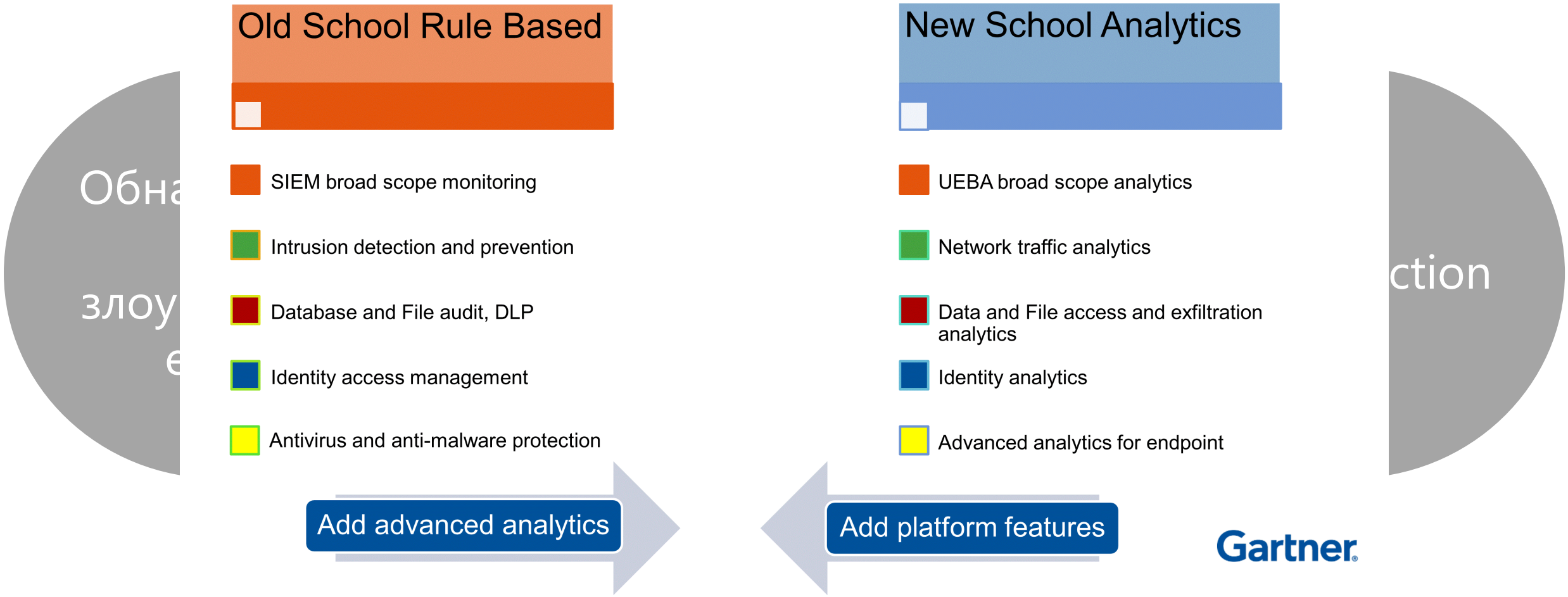
2015

- UEBA or Visibility 2.0

Обнаружение следующего поколения

infotecs

Old School Versus New School Security Products



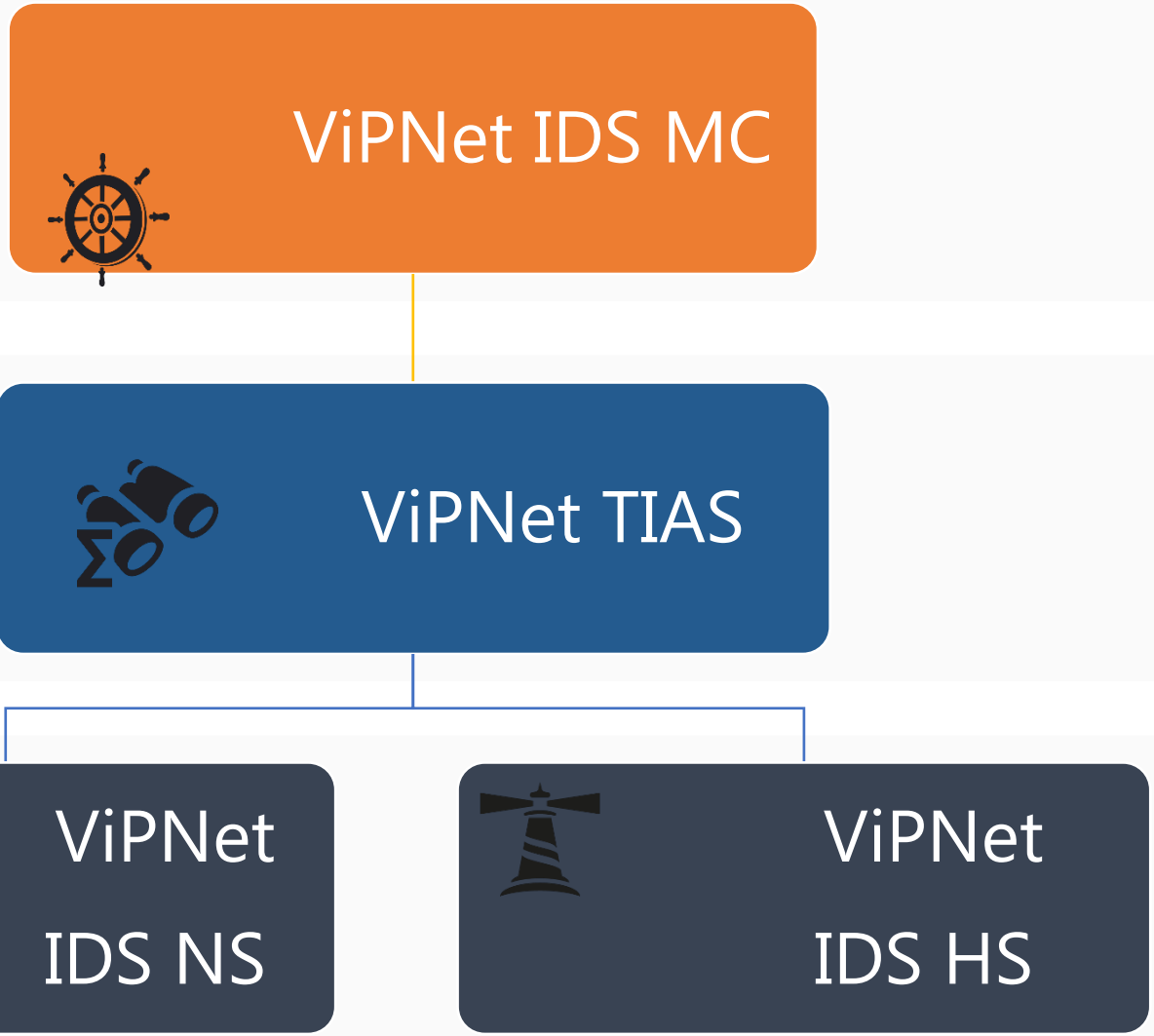
Gartner

Решение по обнаружению угроз и вторжений

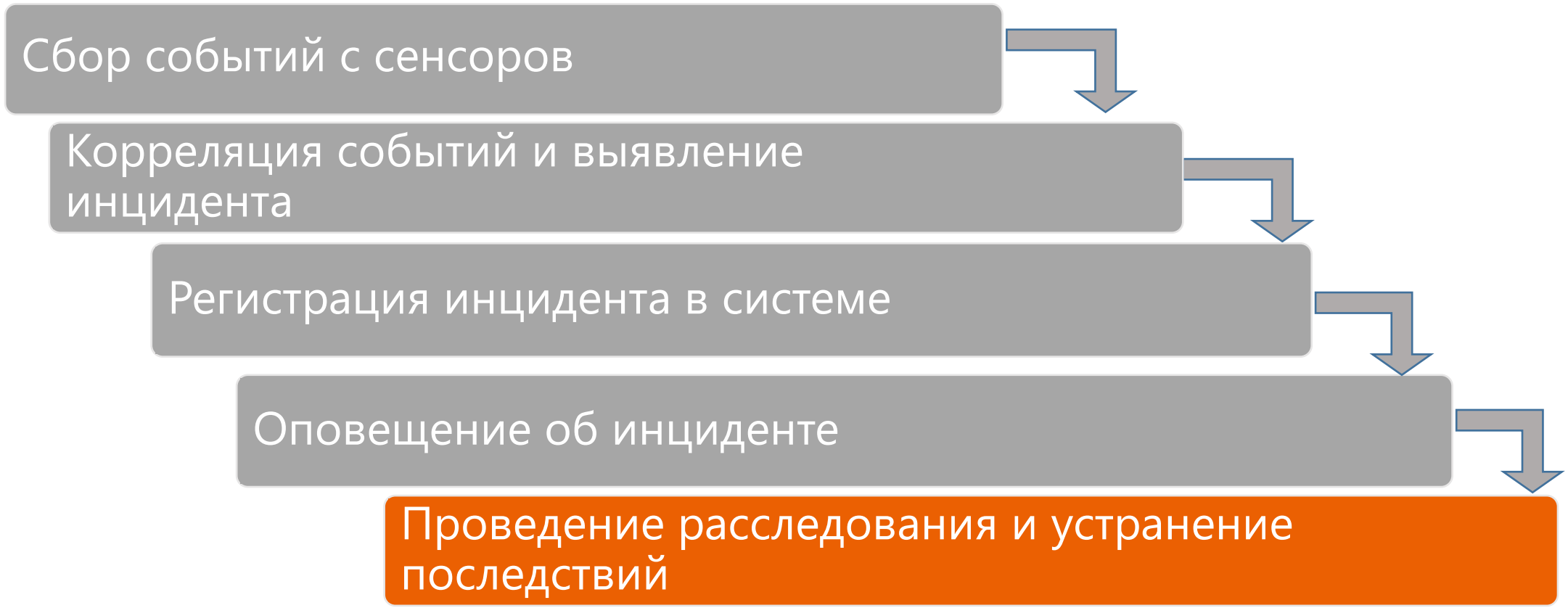
Управление

Аналитика

Сенсоры

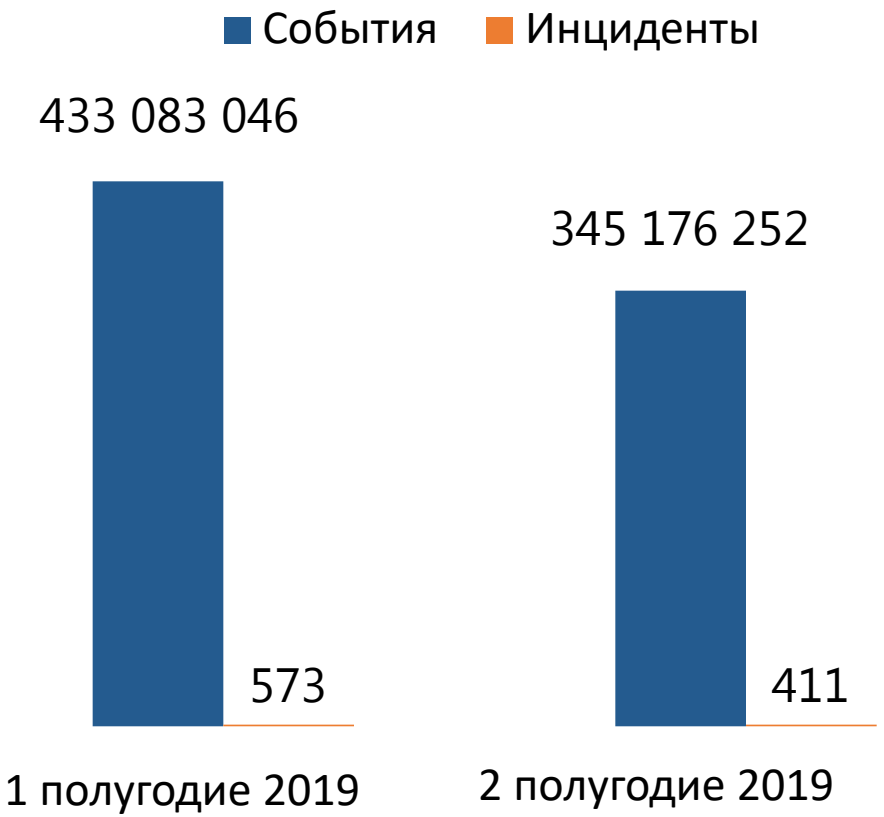


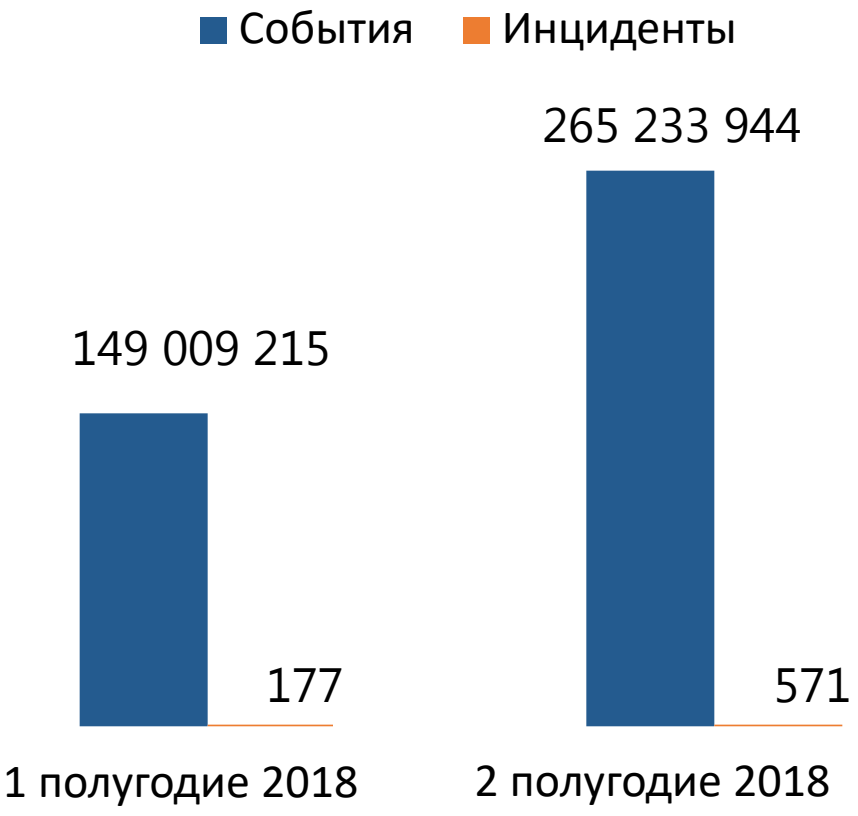
Сценарий обработки событий



Сколько событий обрабатывает SOC

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

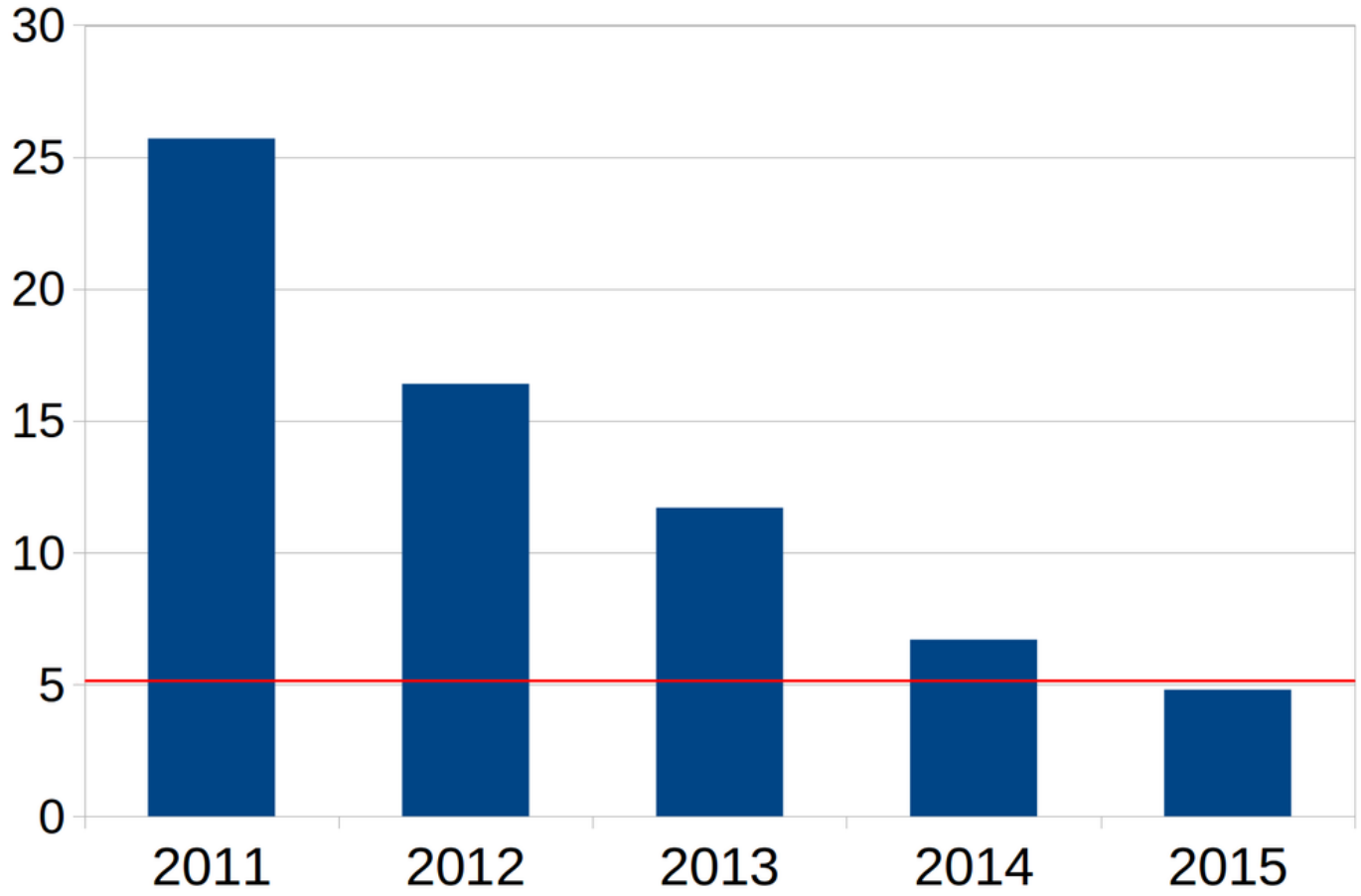




Нам нужна платформа

Что нужно от платформы

Что нас ждет впереди?



Прогресс в автоматической классификации изображений. Процент ошибок, сделанных ИИ по годам. Красная линия — процент ошибок, которые делает обученный человек при выполнении той же задачи.

Что общего у SOC и слоистых коктейлей

- Технологии
- Процессы
- Люди

Цикл зрелости технологий

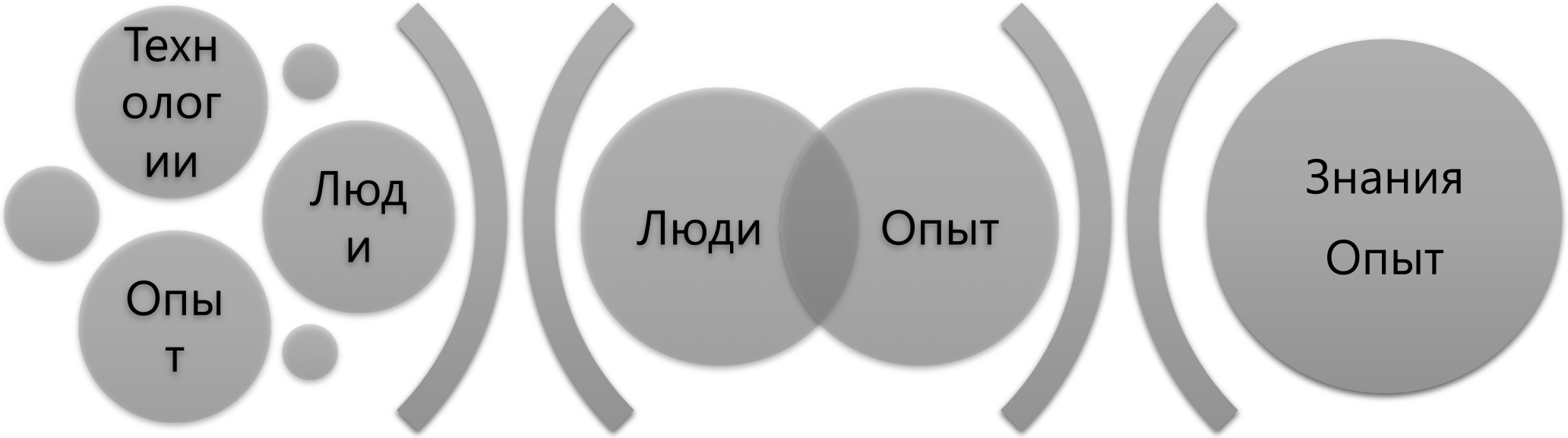
Согласно Gartner
https://habr.com/ru/post/198506/

Для SOC-платформы лучше продукты, а не технологии

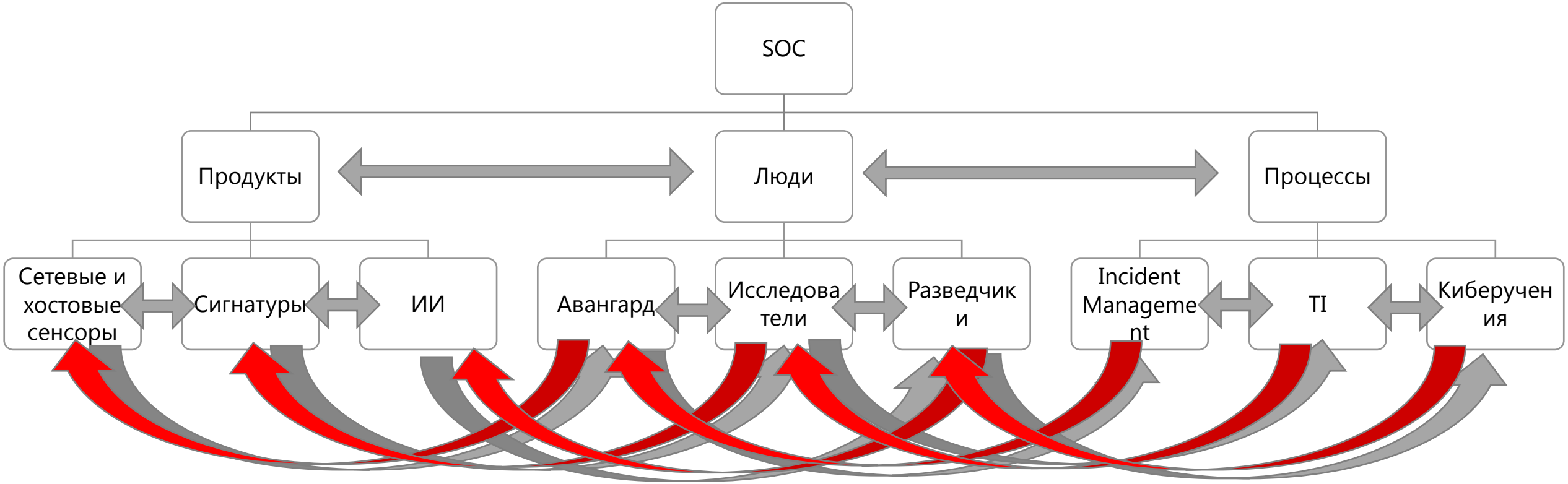
Технология – это утилита, которая помогает улучшить чего-то.

Продукт – это объединение технологии и опыта ее эксплуатации.

Что есть SOC-платформа

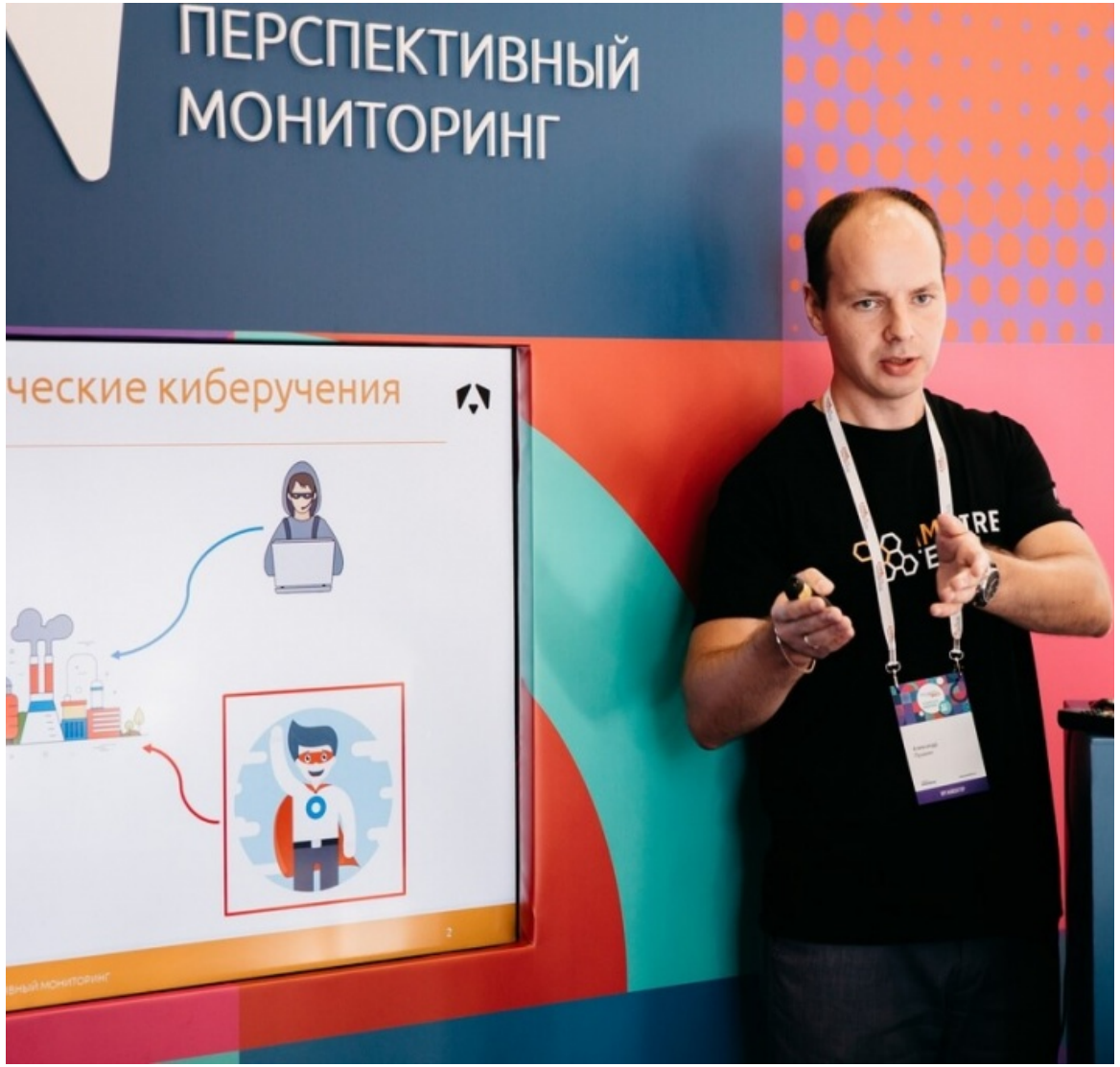


Как это выглядит у нас



Где и как получить экспертизу

- **Второй день 20 ноября**
- **Александр Пушкин**, технический директор, Перспективный мониторинг
- *Киберучения как способ повышения эффективности процессов ИБ*
- Ученье – свет, а киберучения – навыки. Как готовить специалистов так, чтобы мы их потом не переучивали



infotecs

Спасибо!