





Технологии обнаружения компьютерных атак



Методы обнаружения



Обнаружение
злоупотреблени
й



Обнаружение
аномалий

A long time ago...

1984

- Signature detection

2015

- UEBA or Visibility 2.0

Обнаружение следующего поколения

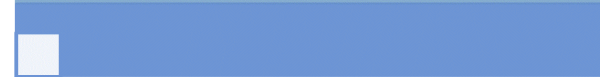
Old School Versus New School Security Products

Old School Rule Based



- SIEM broad scope monitoring
- Intrusion detection and prevention
- Database and File audit, DLP
- Identity access management
- Antivirus and anti-malware protection

New School Analytics



- UEBA broad scope analytics
- Network traffic analytics
- Data and File access and exfiltration analytics
- Identity analytics
- Advanced analytics for endpoint

Обна
злоу
е

ction

Add advanced analytics

Add platform features

Решение по обнаружению угроз и вторжений

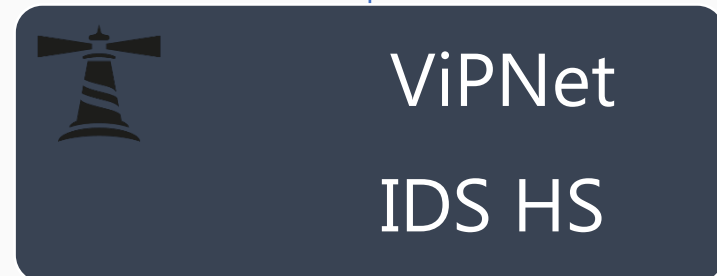
Управление



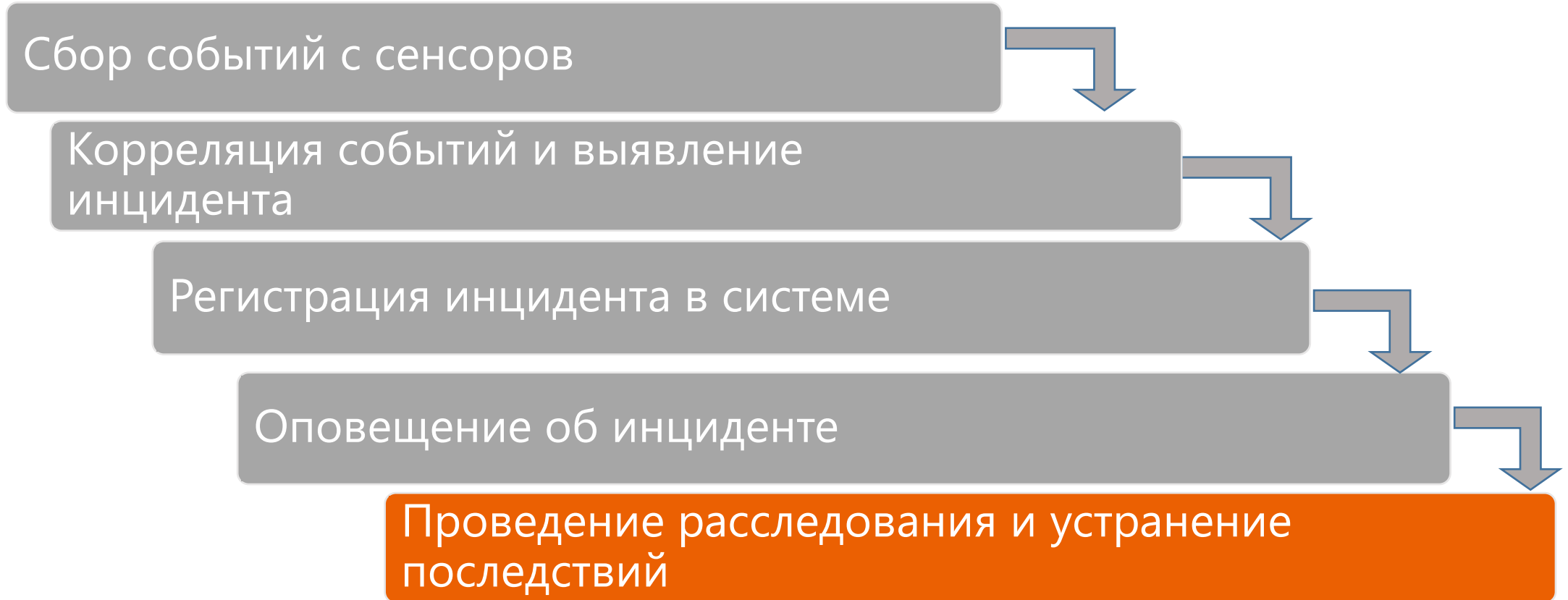
Аналитика



Сенсоры



Сценарий обработки событий



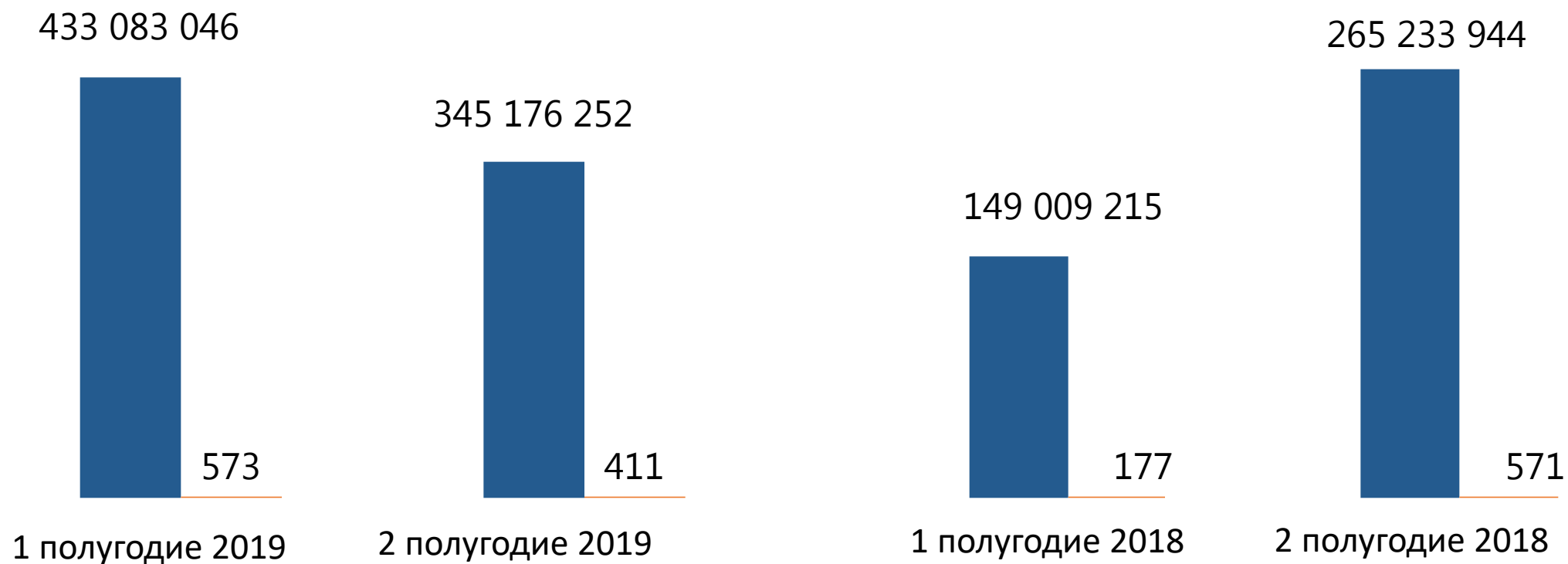
Сколько событий обрабатывает SOC



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

■ События ■ Инциденты

■ События ■ Инциденты





Нам нужна платформа

Что нужно от платформы

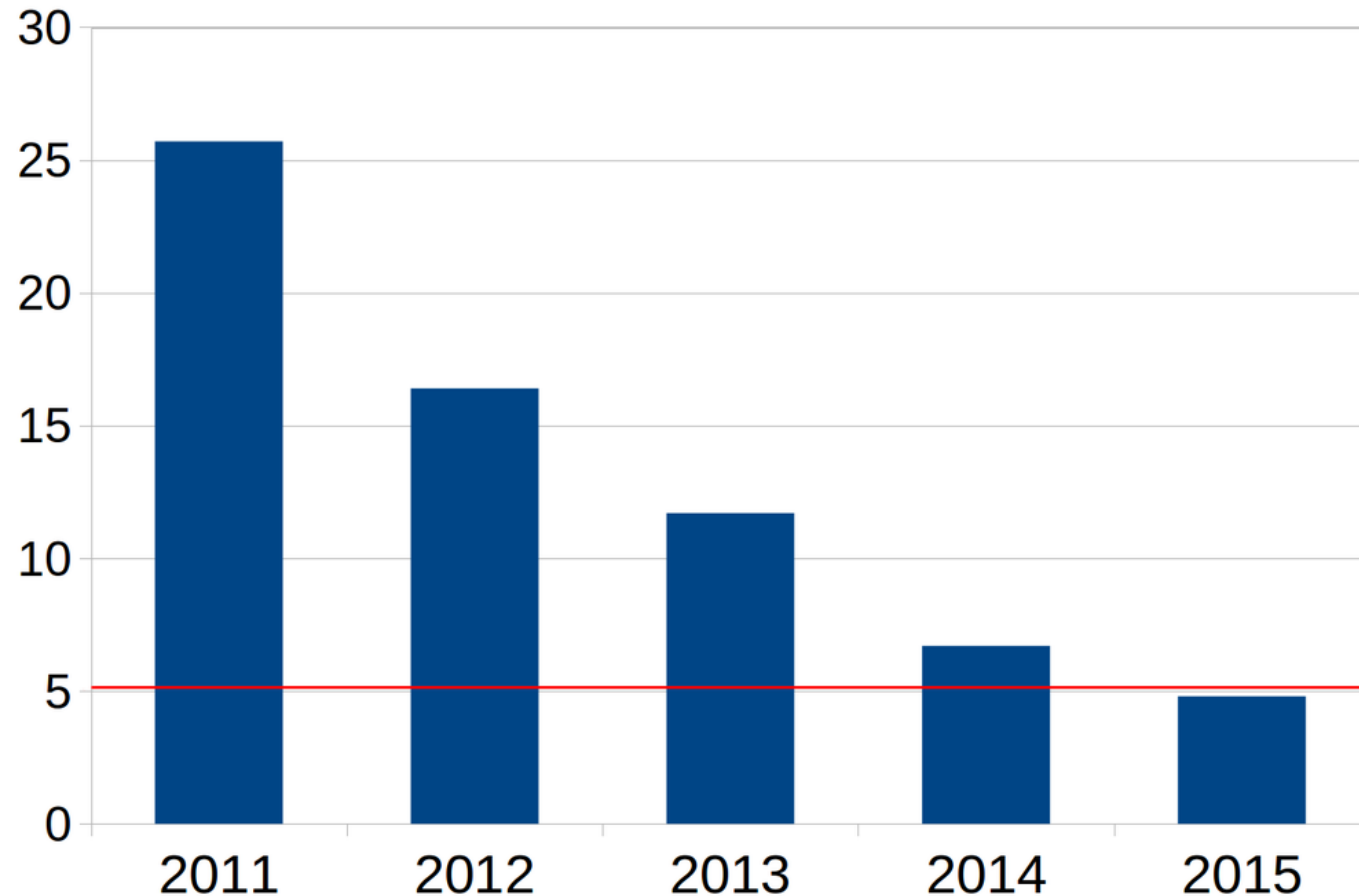
КОГДА ЧЕЛОВЕК С ДЕНЬГАМИ
ВСТРЕЧАЕТ ЧЕЛОВЕКА С
ОПЫТОМ, ЧЕЛОВЕК С ОПЫТОМ
УХОДИТ С ДЕНЬГАМИ, А
ЧЕЛОВЕК С ДЕНЬГАМИ УХОДИТ
С ОПЫТОМ. © АРХИМЕД

RECITE

Made with ♥ by picosy.com



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/>



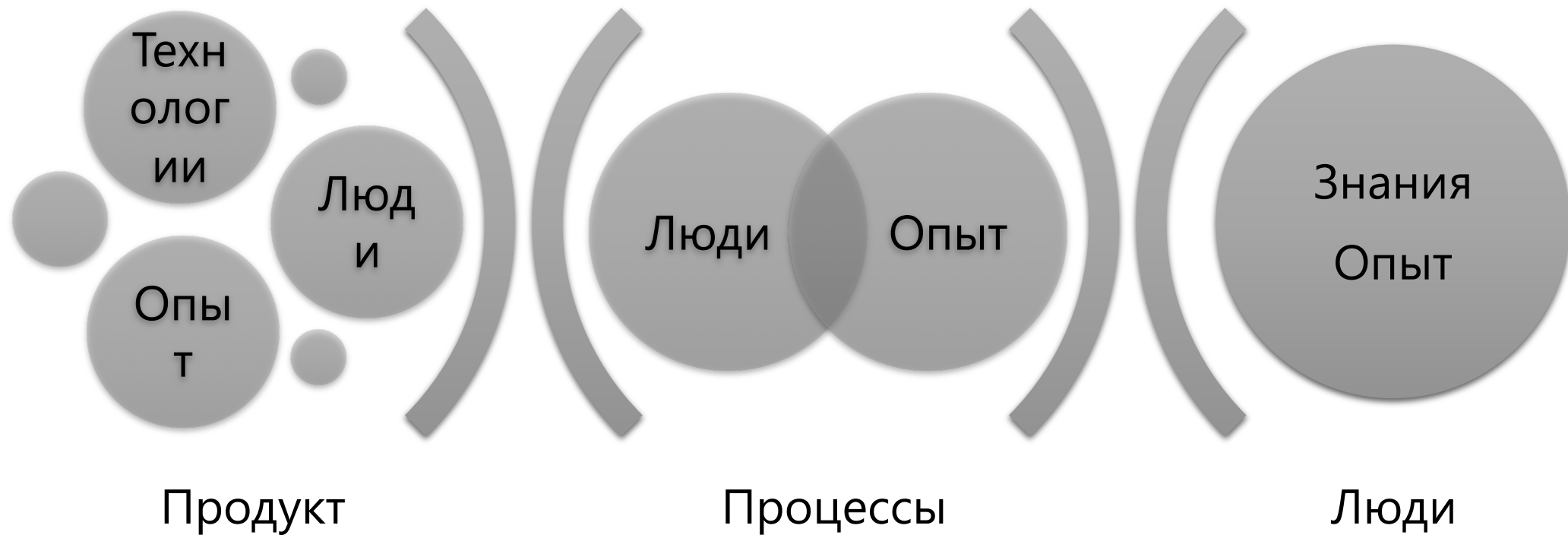
Для SOC-платформы лучше продукты, а не технологии

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

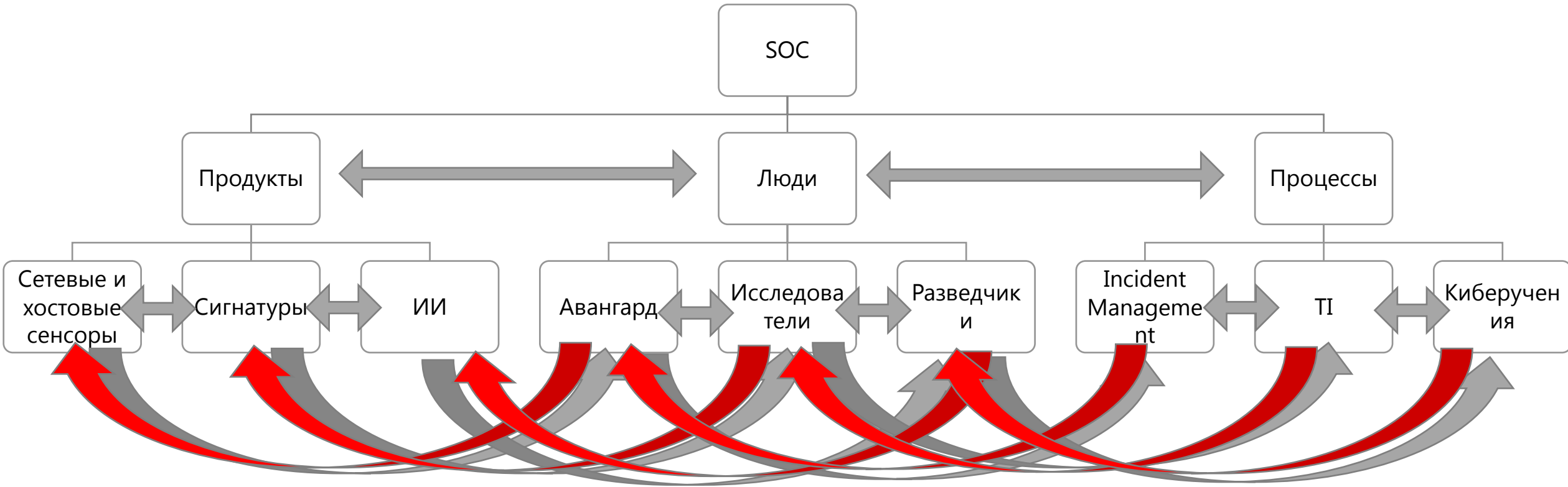
Продукт – это объединение технологии и опыта ее эксплуатации.



Что есть SOC-платформа

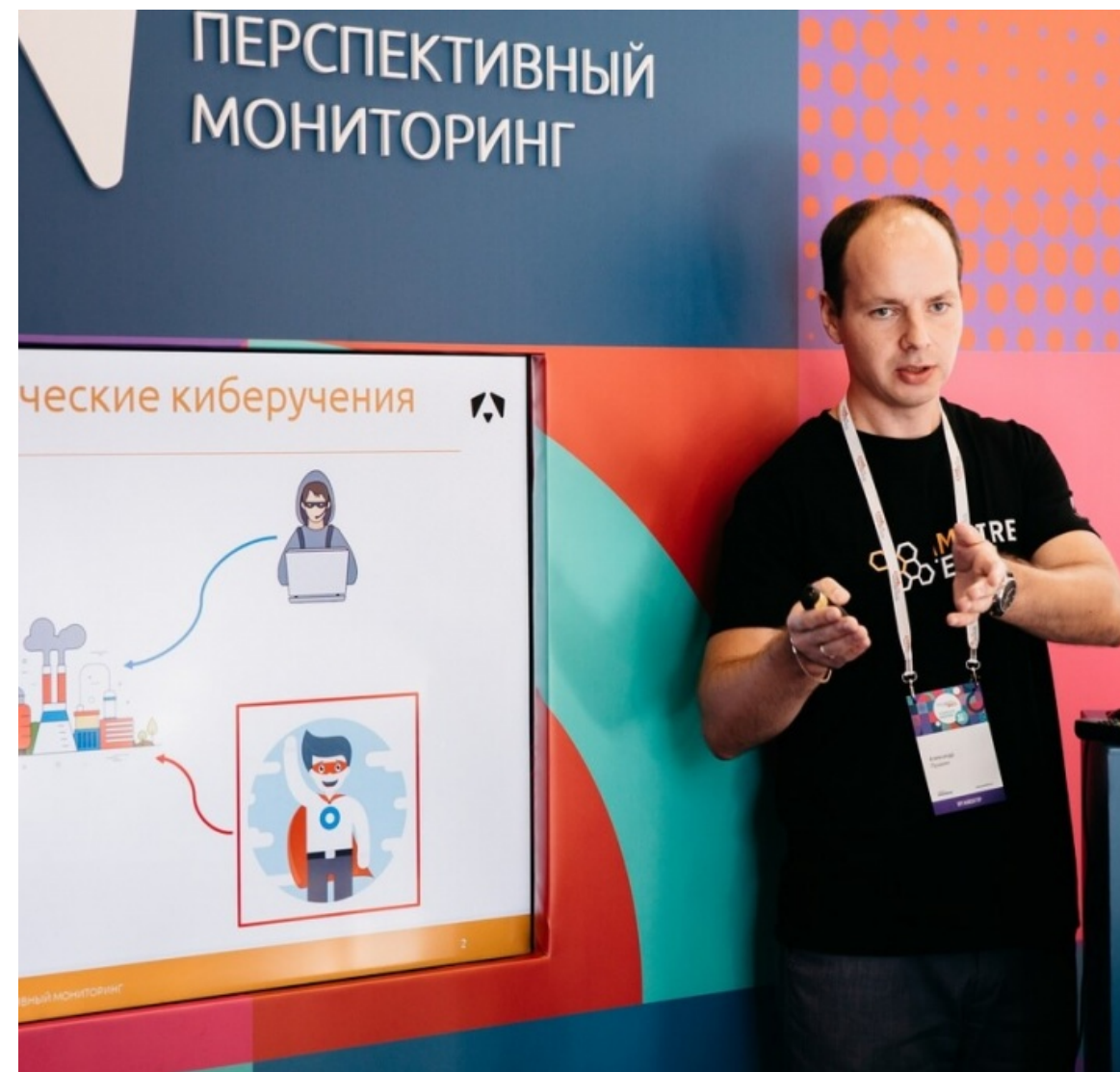


Как это выглядит у нас



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



The logo for 'infotecs' features a stylized orange dot above the letter 'i', followed by a curved orange line above the letters 'f', 'o', and 't'. The word 'infotecs' is written in a bold, dark blue, sans-serif font.

infotecs

A vertical orange line is positioned between the logo and the text.

Спасибо!