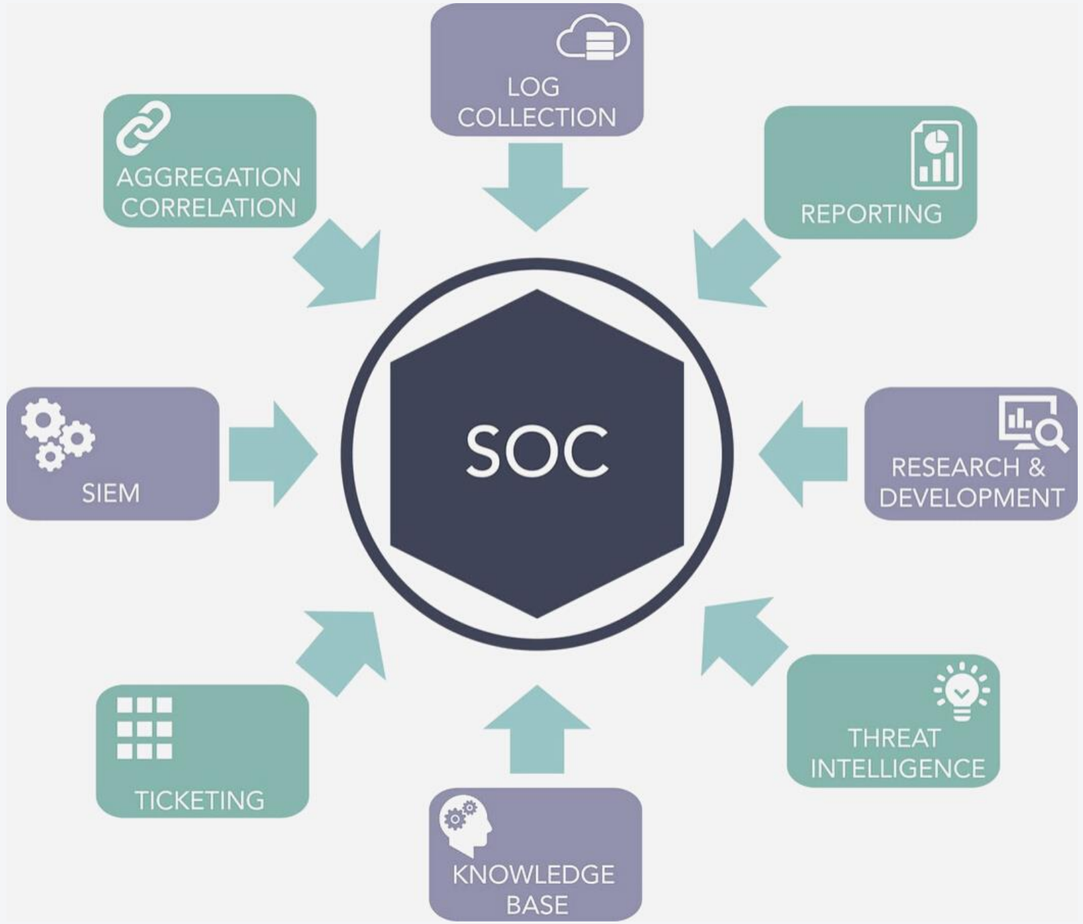
14 АПРЕЛЯ 2021

# СОВРЕМЕННЫЙ ПОДХОД К ПОСТРОЕНИЮ SOC: ПРОЦЕСС, ТЕХНОЛОГИИ, ЛЮДИ

## ВАЖНОСТЬ ПРАВИЛЬНОГО ВЫБОРА И ВЫСТРАИВАНИЯ ВСЕХ КОМПОНЕНТОВ

Антон Фишман, технический директор RuSIEM

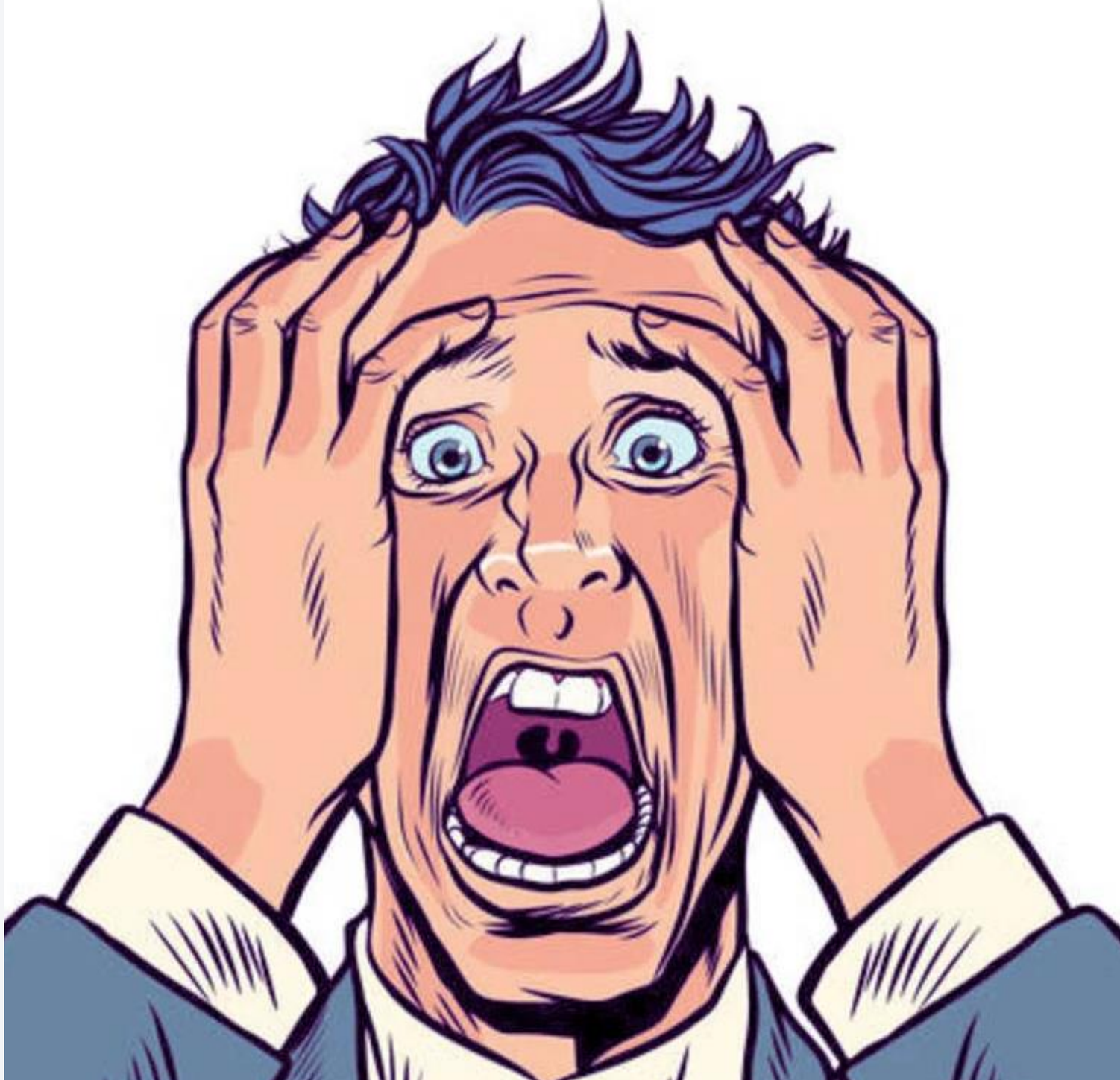



# ЧТО ТАКОЕ SOC*?

Центр мониторинга и реагирования на инциденты информационной безопасности

*SOC - security operations center

# КАК ЭТО ВИДЯТ ОСТАЛЬНЫЕ



# КАК ЭТО НА САМОМ ДЕЛЕ

# ЗАЧЕМ НУЖЕН SOC?

- Непрерывный контроль. Вопрос не в том, взломают или нет, вопрос – когда?
- Рост количества информационных систем и их сложность –> контролировать много каналов
- Централизованная обработка и хранение данных о вторжениях и киберугрозах
- Сами атаки стали комплекснее и требуются процессы и скорость
- Compliance: Критичнее активы – важно защищать

# КАКИЕ БЫВАЮТ SOC?

1

Собственные

2

Гибридные

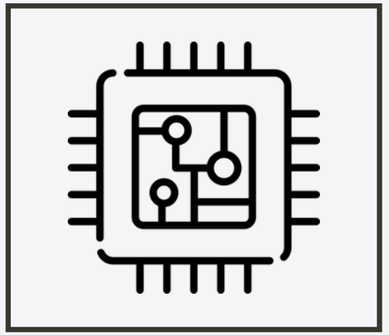
3

Аутсорс

# ИЗ ЧЕГО СОСТОИТ SOC

SOC - механизм, который держится на трех базовых слагаемых:

- команда (персонал)
- процессы (функционал)
- технологии (инструментарий)



# КОМАНДА

## ПЕРВАЯ ЛИНИЯ

Анализ SIEM и первичный анализ

## ВТОРАЯ ЛИНИЯ

Расследование инцидентов

## ТРЕТЬЯ ЛИНИЯ

Глубокий анализ инцидентов и артефактов

## АНАЛИТИКИ SOC

Написание плейбуков, правил корреляции и т.д.)

## СПЕЦИАЛИСТЫ ПО РЕАГИРОВАНИЮ

# Процессы SOC

## МОНИТОРИНГ

Security monitoring

## РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

Отработка происшествий

## УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ

Vulnerability Management

## ФОРЕНЗИКА

Криминалистика

# Процессы SOC

## COMPLIANCE

Соответствие стандартам

## ВНУТРЕННИЙ ПЕНТЕСТ

Оценка защищенности

## THREAT INTELLIGENCE

Киберразведка

## THREAT HUNTING

# ТЕХНОЛОГИИ

- **Security Information and Event Management (SIEM)**
- **SOAR (IRP)**
- **Knowledge Database**
- **Service Desk**
- Vulnerability Management
- Threat Hunting Automation (+EDR)
- Threat Intelligence Feeds
- Threat Intelligence Platform
- Forensic Laboratory (Sandbox)
- Датчики:
  - IDS/IPS
  - FW
  - E-mail
  - Proxy
  - …

- Сбор событий с различных источников
- Нормализация
- Поиск по событиям
- Корреляция
- Управление инцидентами
- Система отчетности
- Управление рисками
- Аналитика
- UEBA
- Управление активами
- Управление уязвимостями
- И многое другое....

# СПАСИБО ЗА ВНИМАНИЕ!

Антон Фишман
технический директор RuSIEM
+7 (903) 158 1572
a.fishman@rusiem.ru