# Почему вам не нужен SOC

## Хаос контролировать невозможно

Kirill Ermakov,
IBM & Jet business breakfast, 2016

# Основы

- Information Security Operations Center
- Центр обработки информации #поИБ
- Часто путают с “Security Monitoring” и “SOC”
- Объединение процессов и технологий
- SOC != ISOC
  - Security Operations Center handles access control, lightning, alarms and vehicle barriers © Wiki
- Тренд последних лет

# Реальность

- Любой, кто купил SIEM, называет его ”SOC”
- Не более чем команда ИБ с парсером логов и движком для корреляции
- Чаще всего даже не понимают, что они мониторят и зачем
- Скорее всего, не имеют опыта во взломе информационных систем

# Cloud solutions

- Сторонняя [redacted] торая купила (разработала) SIEM
- Мониторят [redacted] информацию о событиях 24/7
- Имеют паттерны на типовые кейсы
- Иногда они даже найдут у вас инциденты
- Нет, ну серьезно. Вы правда отдадите кому-то ваши security логи?

# Ок, вы все еще хотите это сделать

- Финансовые затраты на его построение будут больше, чем потенциальные расходы от инцидентов
- Трудоемкость интеграции сравнима с постройкой 2-х чугунных мостов. Как по времени, так и по деньгам
- Вам придется сильно увеличить headcount отдела ИБ

# Как выбрать компоненты

- Что бы вы не купили, оно вам не понравится
- В любом случае без напильника это не работает
- Помните про scalability
- Сделайте в начале дизайн бизнес-процессов, а потом покупайте софт

# Почему он будет работать плохо

- В большинстве компаний полный бардак в ИТ
- Правила из коробки не работают в условиях отсутствия сферической лошади и вакуума
- Если у вас нет инвентаризации, asset management или хотя бы реестра хостов и приложений  - как вы собрались их контролировать?

# Определение аномалий и инцидентов

- Аномалия = отклонение от нормы. Кто знает, что такое норма?
- Инцидент это нарушение каких-то правил/политик. Для этого нужно сначала их создать.
- А что, контроль изменений уже внедрен?

# Перейдем к внедрению

- Если вы сами не знаете в деталях, как работают ваши системы и приложения, интегратор точно это не узнает за вас

- Ресурсные потребности SIEM сопоставимы с (не)большим процессингом

- Автодискавери и автопарсинг сломаются

# Первый запуск

- Вы узнаете, что у вас миллион инцидентов
- Самые важные будут – ICMP Flood и ”У вас SSH в сети!”
- Подключили к мониторингу периметр? Скоро у вас кончится место на дисках
- Но есть и плюс – вы узнаете, кто в вашей компании до сих пор пользуется IRC

# Через год

- Ваша команда, наконец, научится его использовать
- Вы удалите все правила “из коробки” и “от интегратора”
- Заставите отдел эксплуатации провести, наконец, инвентаризацию
- Будете знать досконально, как этот комбайн работает внутри
- Будете смотреть за трендами, а не за событиями

# Через два года

- Вы начнете отключать лишние источники событий
- Наконец разберетесь, как устроена база и API вашего SIEM
- Сделаете свои консоли мониторинга
- Перестанете пытаться реагировать на ”TCP Port scan”
- Введете KPI и ”Red Team” учения для проверки своего ISOC

# SOC overview

- Очень дорого, но потенциально очень круто
- Инвестировать в людей эффективнее, чем в продукты
- Работает только в условиях здоровых процессов в компании и минимального порядка в ИТ
- Чем больше хаоса, тем дороже (I)SOC и дороже люди, обеспечивающие его работу

# Почему я так уверенно говорю это?

- Два года с IBM qRadar
- 28 000 событий в секунду
- 5 человек мониторят события
- 41 сервер мониторинга
- 2 500 хостов
- /16 сеть в мир
- Been there, done that

# +/-

- qRadar неплохой софт, если знать как его готовить
- qFlow, vFlow не работают
- Собственный SOC позволяет не прозевать момент, когда уже все плохо
- Интегратор может помочь написать правила парсинга, но не правила реагирования
- Получилось поймать настоящие инциденты

# Ну и что собственно делать?

- Наводить порядок в ИТ-хозяйстве
- Строго регламентировать ”Кто-куда-зачем и почему”
- Разбираться в том, как действуют хакеры
- Мониторить то, что нужно и важно, а не все подряд
- Не верить, что софт сделает что-то за вас
- Нанять практических безопасников в команду

# Спасибо

Вопросы?

isox@vulners.com