JETSECURITY
CONFERENCE 2018

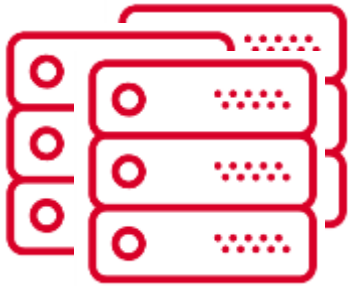
Практика создания SOC

Дмитрий Кузнецов,
Positive Technologies

С чего мы начинали

JETSECURITY CONFERENCE 2018

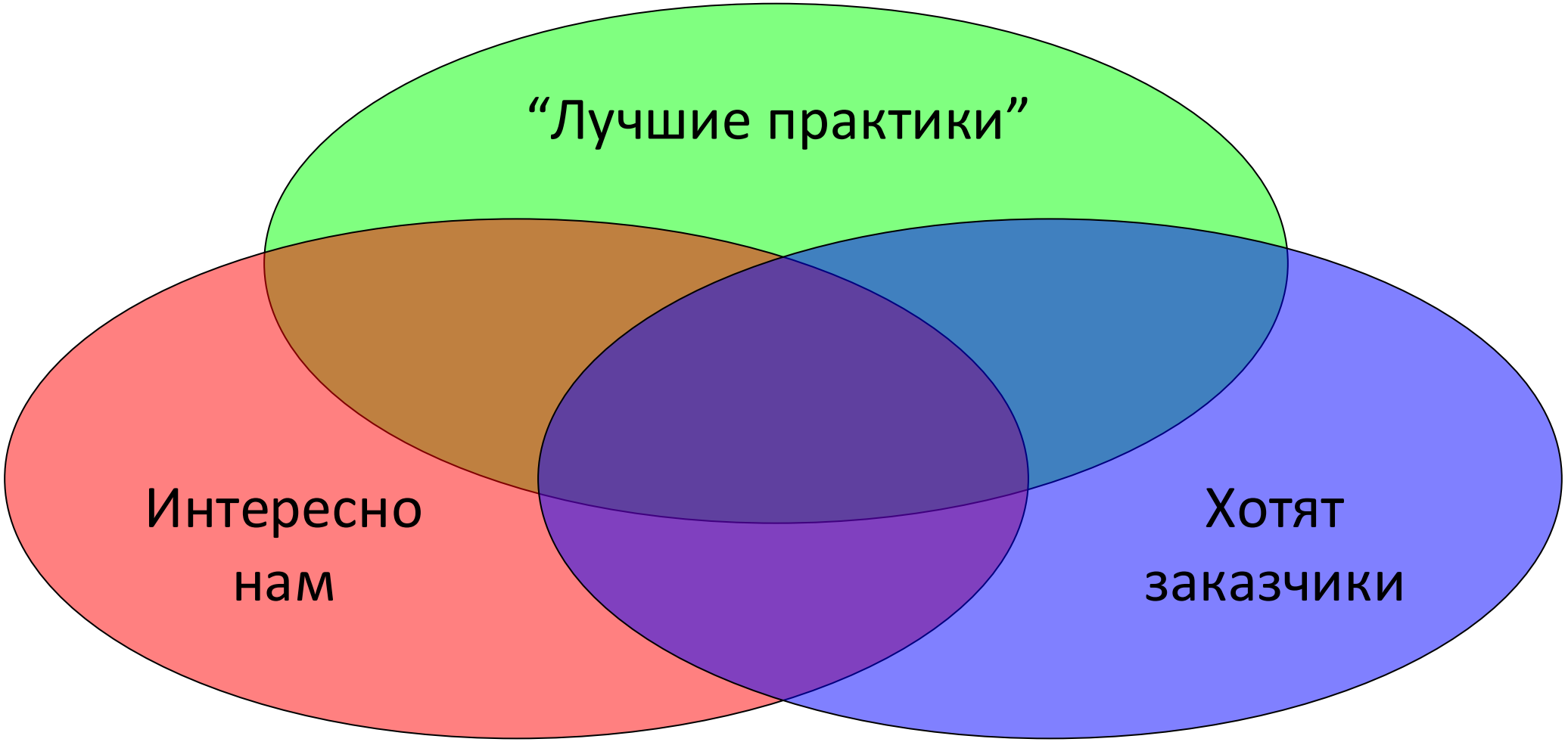
Есть люди, но нет процессов



Много средств защиты, нет единого понимания

Высокий технический уровень

“Не все йогурты одинаково полезны”



CERT или SOC?

JETSECURITY CONFERENCE 2018

Сходства

- “Единое окно”
- Отслеживание уязвимостей
- Стандартизация “безопасных конфигураций”
- Обнаружение атак
- Реагирование на атаки

Различия

- SOC проводит оценку защищенности индивидуальных ИС
- CERT не работает “в поле”
- SOC обеспечивает полное покрытие ИС, CERT – только периметр
- Для SOC характерна операционная деятельность, для CERT - консалтинг

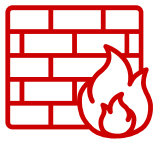
Шаг 1

JETSECURITY CONFERENCE 2018

1

Обеспечения защищенности периметра от типовых атак

MaxPatrol 8



PT Application Firewall

MaxPatrol SIEM

Сервис Advanced Border Control

- Сбор и обработка сведений об информационных ресурсах на периметре: инвентаризационная + справочная информация
- Сбор и обработка сведений о состоянии защищенности информационных ресурсов на периметре: уязвимости
- Обнаружение атак на публичные сервисы

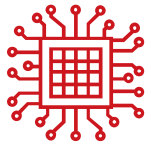
Шаг 2

JETSECURITY CONFERENCE 2018

2

Обеспечения защищенности внутренней инфраструктуры от типовых атак

MaxPatrol 8



PT Network Attack Discovery

MaxPatrol SIEM

- Сбор и обработка сведений об информационных ресурсах: инвентаризационная + справочная информация
- Сбор и обработка сведений о состоянии защищенности информационных ресурсов: уязвимости
- Анализ сетевого трафика
- Анализ событий безопасности

Шаг 3

JETSECURITY CONFERENCE 2018

3

Обеспечения защищенности инфраструктуры от нетиповых атак

PT Application Inspector

PT MultiScanner

- Анализ исходного кода
- Ретроспективный анализ трафика
- Динамический анализ передаваемых в трафике объектов на наличие ВПО

К – команда!

JETSECURITY CONFERENCE 2018

Руководитель SOC: руководит соком

1-я линия:
Первичная оценка инцидентов, отработка ложных срабатываний, простейшая обработка по плейбукам

2-я линия:
Глубокое расследование инцидентов

3-я линия:
Глубокий анализ артефактов инцидентов

Аналитики: пишут плейбуки, TI

Так же двигаемся постепенно!

JETSECURITY CONFERENCE 2018

1. Руководителя SOC берем изнутри
2. 1-я линия набирается быстро, плейбуки в IRP платформе
3. 2 и 3 линия на первом этапе – на стороне PT

Одновременно с этим взращиваем команду у себя внутри, правильно мотивируя

JETSECURITY
CONFERENCE 2018

Спасибо за внимание!

БОЛЬШЕ ЧЕМ БЕЗОПАСНОСТЬ