Специфика мониторинга и управления инцидентами кибербезопасности АСУ ТП

Даренский Дмитрий

Руководитель практики промышленной кибербезопасности

ptsecurity.com

Заблуждения серьёзных людей

Не запугивайте, а покажите статистику

Да кому мы нужны! Нас атаковать нет смысла

У нас АСУ ТП изолирована, воздушный зазор

Ну и где ваши хакеры? У нас как работало всё так и работает!

Чтобы взломать АСУ ТП нужно быть семь пядей во лбу!

Я свою АСУ ТП знаю как свои пять пальцев. У нас вирусов нет!

Вопрос не в том, взломают или нет вопрос в том - когда

В 2 раза

выросло число компаний, которые стали жертвами целевых атак в 2017 году

90%

компаний взламываются от одного до пяти дней

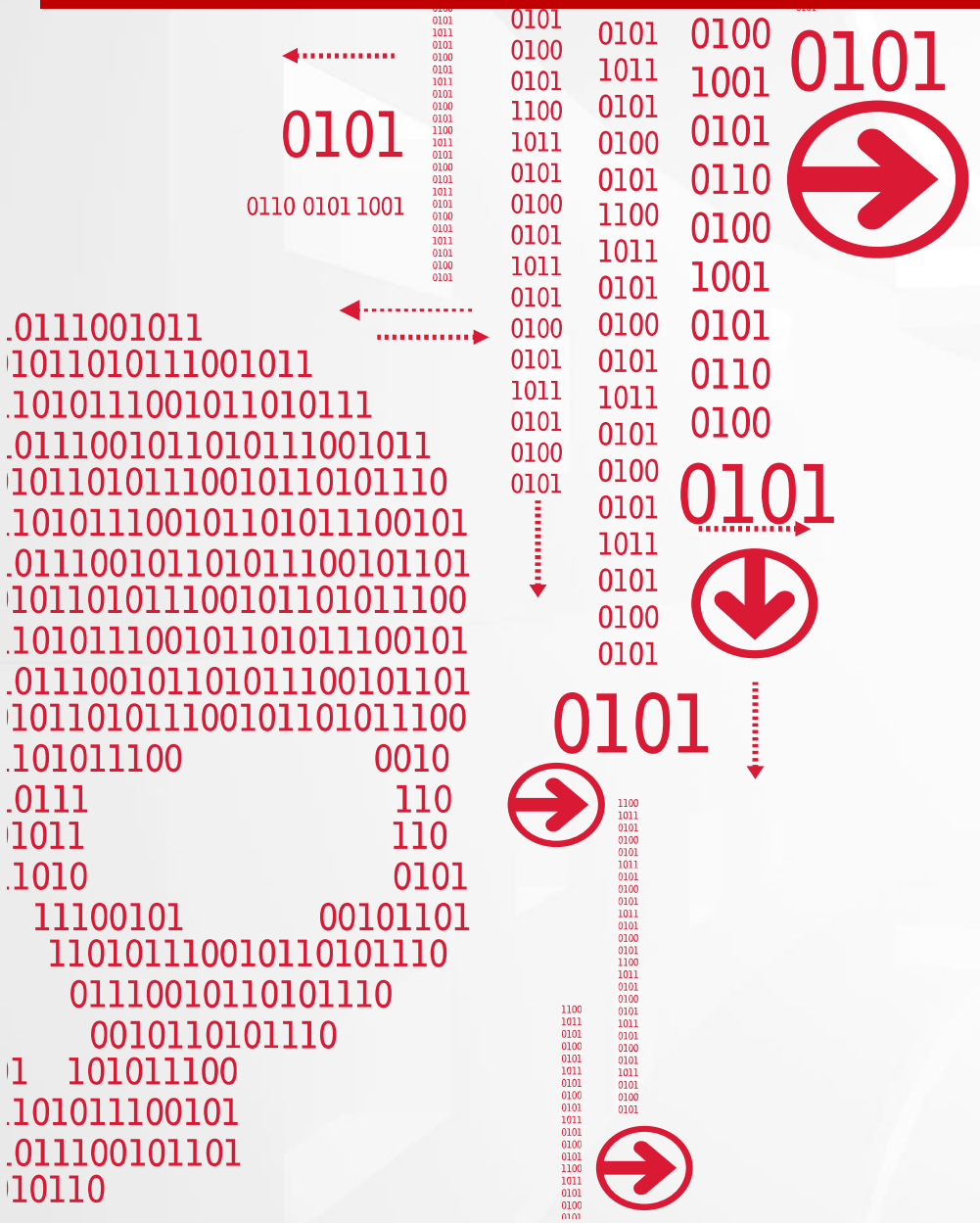
9 из 10

жертв не замечают факт взлома

200 дней

составляет среднее время обнаружения компрометации

Активные хакерские группировки



Неизвестные китайские группировки

Страна: Китай

Основной фокус:
Целевые атаки
на правительство РФ
и компании ВПК сектора

SongXY

Страна: Китай

Основной фокус:
оборонные
и промышленные
предприятия

APT37

Страна: Северная Корея

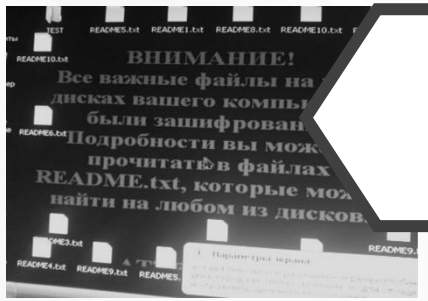
Основной фокус:
государственные учреждения, оборонно-промышленный комплекс, ВПК, промышленность, аэрокосмическая область

Equation

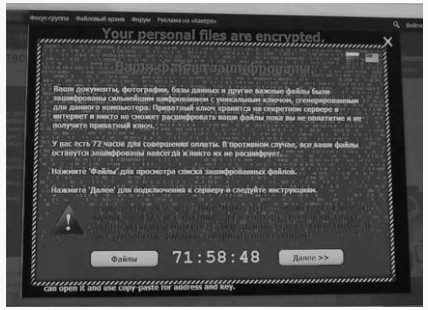
Страна: США

Основной фокус:
государственные учреждения, ВПК

Контекст инцидента



«Безопасники»- инцидент это нарушение свойств безопасности информации, обрабатываемой в автоматизированной системе



«Асушники» - инцидент это нарушение режимов функционирования системы или нарушение технологического процесса

Специфика управления инцидентами в АСУ ТП

ptsecurity.com

Кто ближе к истине? Закон!!!

Компьютерный инцидент (ФЗ 187)

«Асушники»

«Безопасники»

факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, **и (или) нарушения безопасности обрабатываемой** таким объектом **информации**, в том числе произошедший в результате компьютерной атаки.

АСУ ТП + Классические СЗИ=???

Классические меры защиты?

ДА, НО НЕТ:

- Конфликты средств защиты и основного ПО
- Ложные срабатывания
- Проблемы с установкой обновлений
- Функции активной защиты не используются, даже если они есть
- Сложности выявлением и расследованием инцидентов
- Размытые зоны ответственности между специалистами ИТ, ИБ и АСУ ТП

АСУ ТП + SIEM=???

1. Сегодня для любого SOC/SIEM АСУ ТП клиента это «слепое пятно»
2. Специалистам SOC для принятия решения по инциденту требуется глубокий и специфичный контекст
3. SIEM сложно «научить» коррелировать события прикладного характера АСУ ТП
4. На большинстве предприятий процессы реагирования на инциденты кибербезопасности АСУ ТП отсутствуют

С чего начинать?

ptsecurity.com

С чего начать? Шаг 1

Поставить на мониторинг технологическую сеть АСУ ТП

PT ISIM

…или аналоги, заслуживающие доверия

Результат:

- Формируется реальное представление о состоянии защищенности АСУ ТП
- Возможность оперативно реагировать на самые критичные проблемы безопасности
- Появляется источник информации об инцидентах и угрозах

С чего начать? Шаг 2

Постоянно и тщательно наблюдать за активами инфраструктуры предприятия

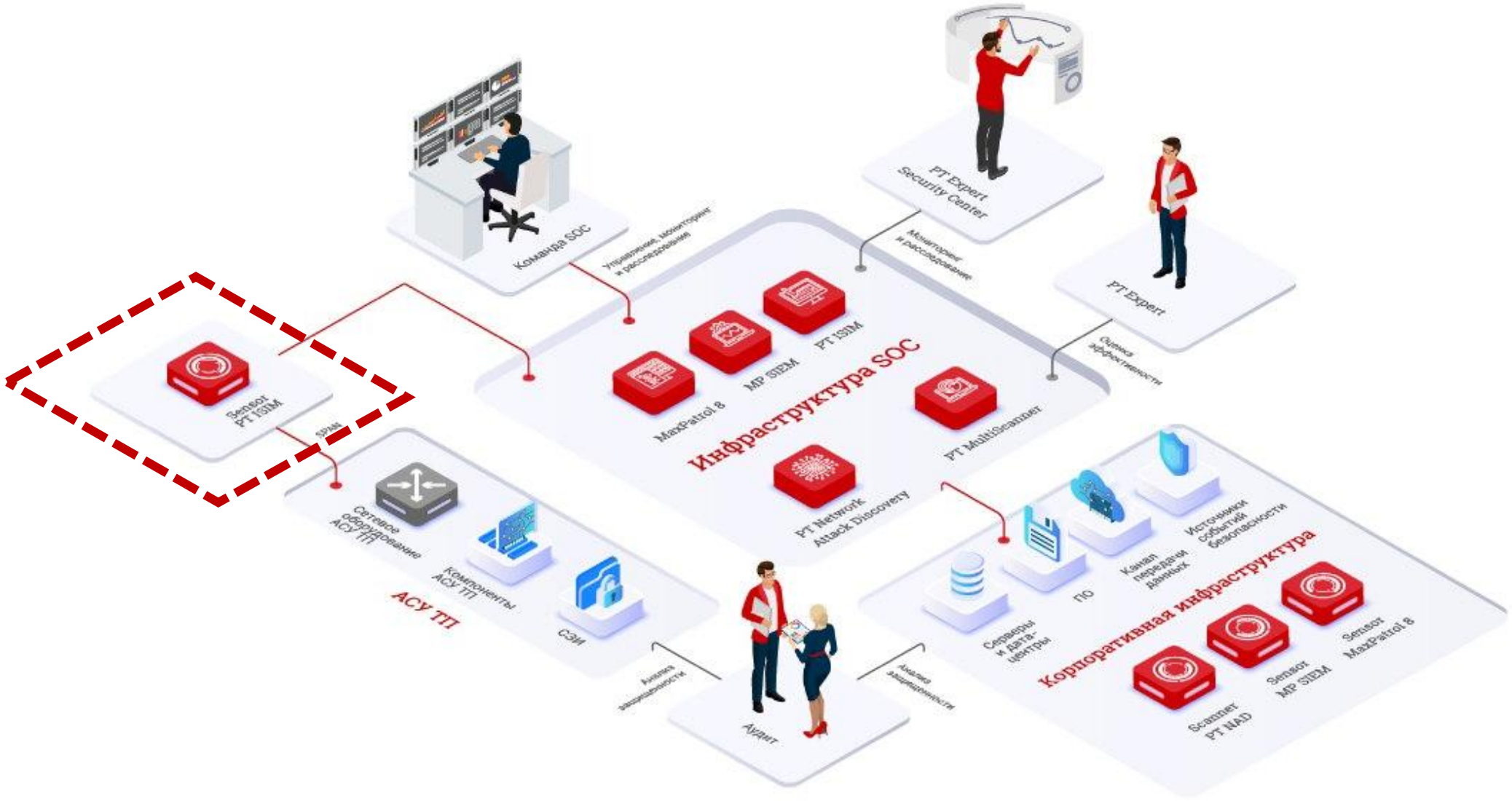
→ **MP SIEM**

…или аналоги, заслуживающие доверия

Результат:

- Под контролем вся ИТ инфраструктура предприятия целиком, включая АСУ ТП
- Попытка Взлома, атака, инцидент оперативно выявляется и реагирование выполняется в рамках единого процесса
- Своевременное принятие компенсирующих мер и минимизация ущерба.

Как это выглядит?



О нас

ДЕЛАЕМ:

Аудиты безопасности	Хакеры знают, как вас можно взломать	Узнайте реальные вектора атак на ваши системы
Расследование атак	Хакеры сидят внутри в среднем 197 дней	Поможем выявить и локализовать взломанные узлы и сервисы
Продукты безопасности	Строим центры мониторинга для выявления атак на все компоненты инфраструктуры	Комплексная защита АСУ ТП и корпоративной сети

Выявляем и уведомляем производителей оборудования о найденных нами уязвимостях

Создаем совместные решения с производителями систем промышленной автоматизации

15
лет опыта исследований и разработок

700
инженеров по ИБ, разработчиков, аналитиков и других специалистов

250
экспертов в нашем исследовательском центре безопасности — одном из крупнейших в Европе

POSITIVE TECHNOLOGIES

Свяжитесь с нами:

+7 495 744 01 44

sales@ptsecurity.com

ptsecurity.com