SOC-FORUM ASTANA 2017

Ядро SOC

Алексей Качалин

POSITIVE TECHNOLOGIES

ptsecurity.ru

Компетенции, реализованные в продуктах и сервисах

MaxPatrol **MaxPatrol** SIEM	Мониторинг безопасности на всех уровнях информационной системы, а также сбор событий и анализ состояния системы
PT Multiscanner	Выявление вредоносных файлов, полученных по почте и хранящихся в корпоративных базах, десятками антивирусов
Сервисы	**Тест на проникновение** **Анализ защищенности** **Анализ угроз и расследование инцидентов**

PT Application Inspector **PT** Application Firewall	Защита веб-порталов и бизнес-приложений на этапе разработки и эксплуатации
PT ISIM **PT** SS7 Attack Discovery	Выявление атак на критически важные системы телекомов и промышленных предприятий

Слагаемые успеха SOC

+Технологии

+Люди

+Методики

SOC

??? Что первично ???

ИБ – есть проблемы?

POSITIVE TECHNOLOGIES

(Вечно) Актуальные проблемы

Инвентаризация

- состав системы – что будут атаковать
- чем рискуем, активы?

Уязвимости

- конфигурации
- компонентов

Наблюдаемость и контроль

- мониторинг ИБ
- контроль штатных активностей (выявление аномалий)

Осведомленность об угрозах

- ландшафт угроз
- новые угрозы
- покрытие технологий

Специфика активов и процессов

- специфика бизнес процессов, «свой» код
- каждая организация уникальна

(Вечно) Актуальные проблемы

Инвентаризация

- состав системы – что будут атаковать
- чем рискуем, активы?

Уязвимости

- конфигурации
- компонентов

Наблюдаемость и контроль

- мониторинг ИБ
- контроль штатных активностей (выявление аномалий)

Осведомленность об угрозах

- ландшафт угроз
- новые угрозы
- покрытие технологий

Специфика активов и процессов

- специфика бизнес процессов, «свой» код
- каждая организация

ДИНАМИКА

(Вечно) Актуальные проблемы

Интеграция контролей безопасности

Инвентаризация

- состав системы – что будут атаковать
- чем рискуем, активы?

Уязвимости

- конфигурации
- компонентов

Наблюдаемость и контроль

- мониторинг ИБ
- контроль штатных активностей (выявление аномалий)

Осведомленность об угрозах

- ландшафт угроз
- новые угрозы
- покрытие технологий

Специфика активов и процессов

- специфика бизнес процессов, «свой» код
- каждая организация

ДИНАМИКА

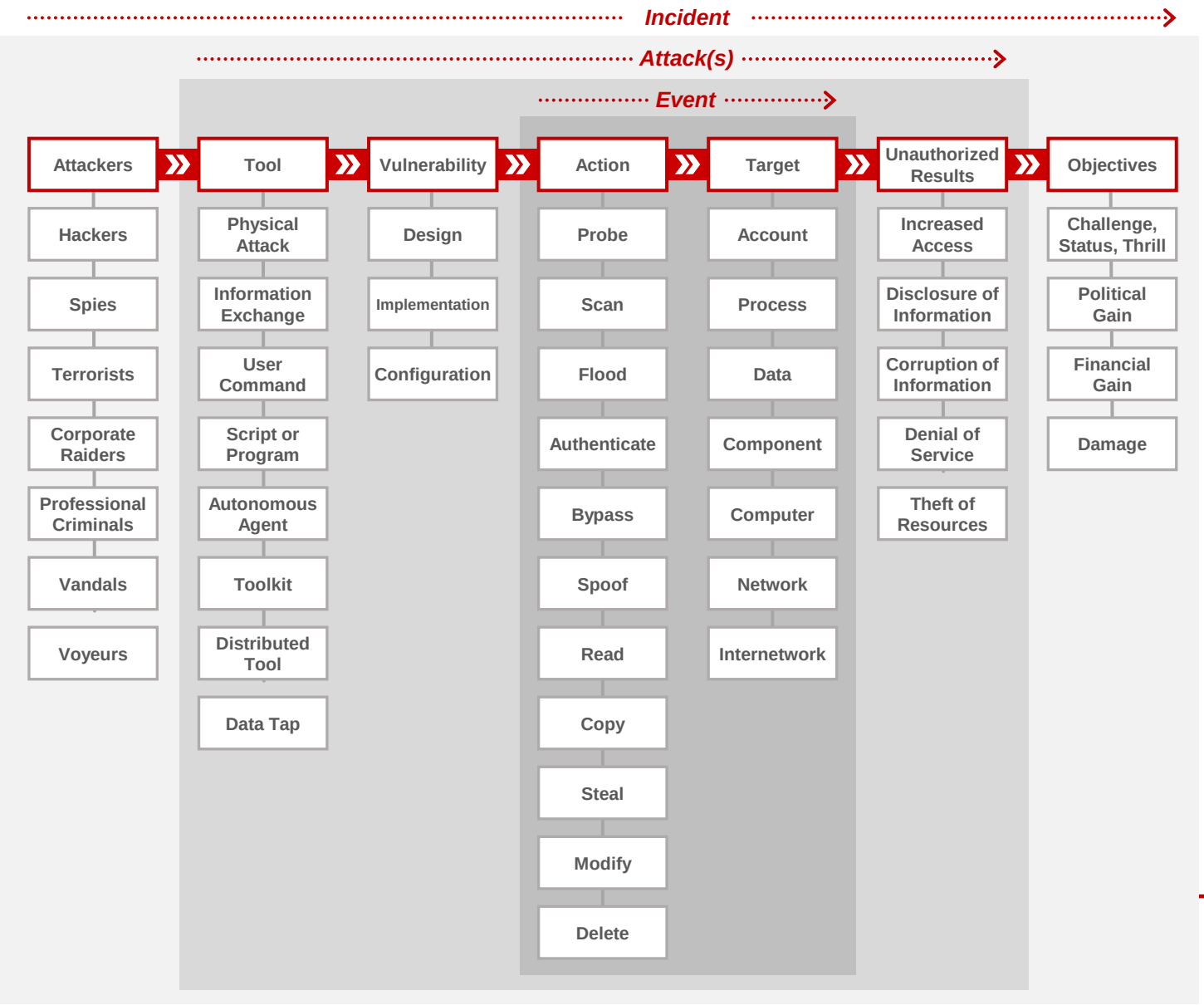
Эффективный SOC?

POSITIVE TECHNOLOGIES

Симптомы здорового SOC

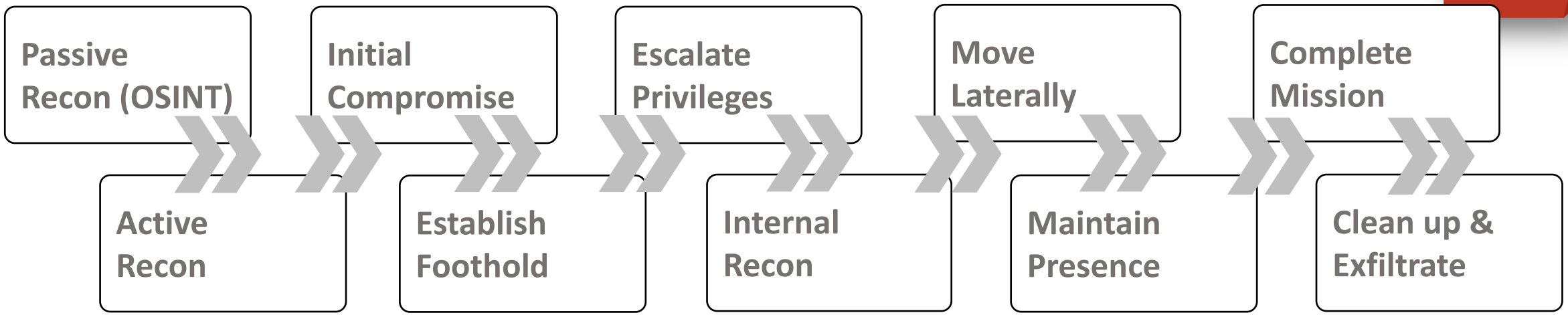
- Обнаружение угроз. На каждом шаге *killchain*
- Фиксировать каждое событие – ничто не упущено
- Сбор материалов и доказательств для расследования
- Эффективное противодействие инцидентам
- Управление инцидентами – прозрачность + коммуникации
- Постоянная автоматизация процессов, оптимизация операций

Знать себя: от событий безопасности к инцидентам



- События
  - Активы
  - Наблюдаемость изменений
- Атаки
  - Уязвимости
- Инциденты
  - Цели и тактика атакующего

Знать врага: killchain - важен каждый шаг

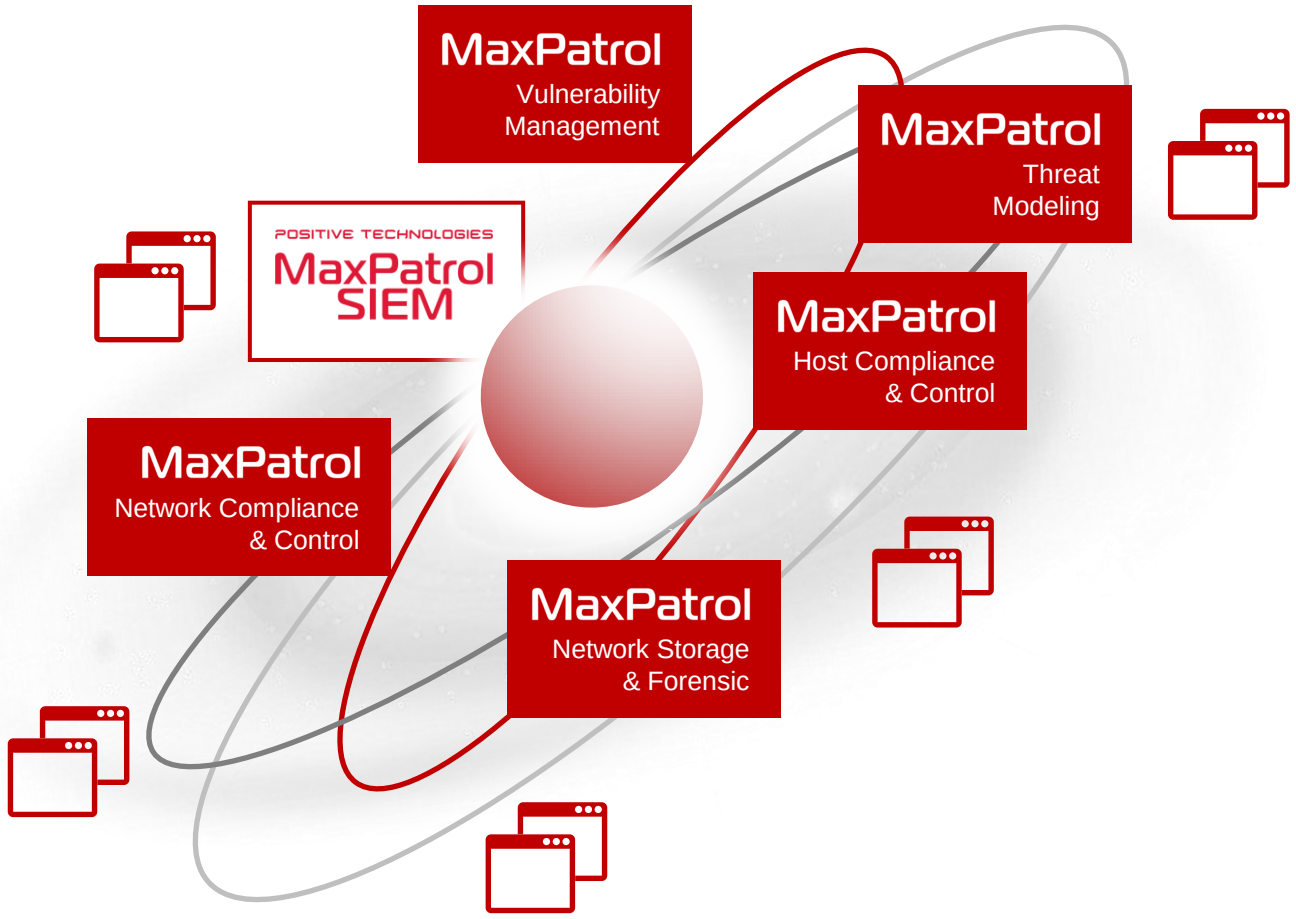


- Протяженность во времени: от секунд до месяцев
- Область видимости: от пассивных действий до вмешательства в работу СЗИ
- Эффективное противодействие - не борьба с симптомами

Ядро платформы MaxPatrol

MaxPatrol SIEM

- 13 лет масштабных тестов на проникновение
- Сотни найденных 0-day уязвимостей в год
- Ежедневные анализы реальных инциденты ИБ
- Positive Expert Security Center – всегда на переднем крае
- Аналитика и моделирование атак
- Прототипирование и испытание технологий



MaxPatrol

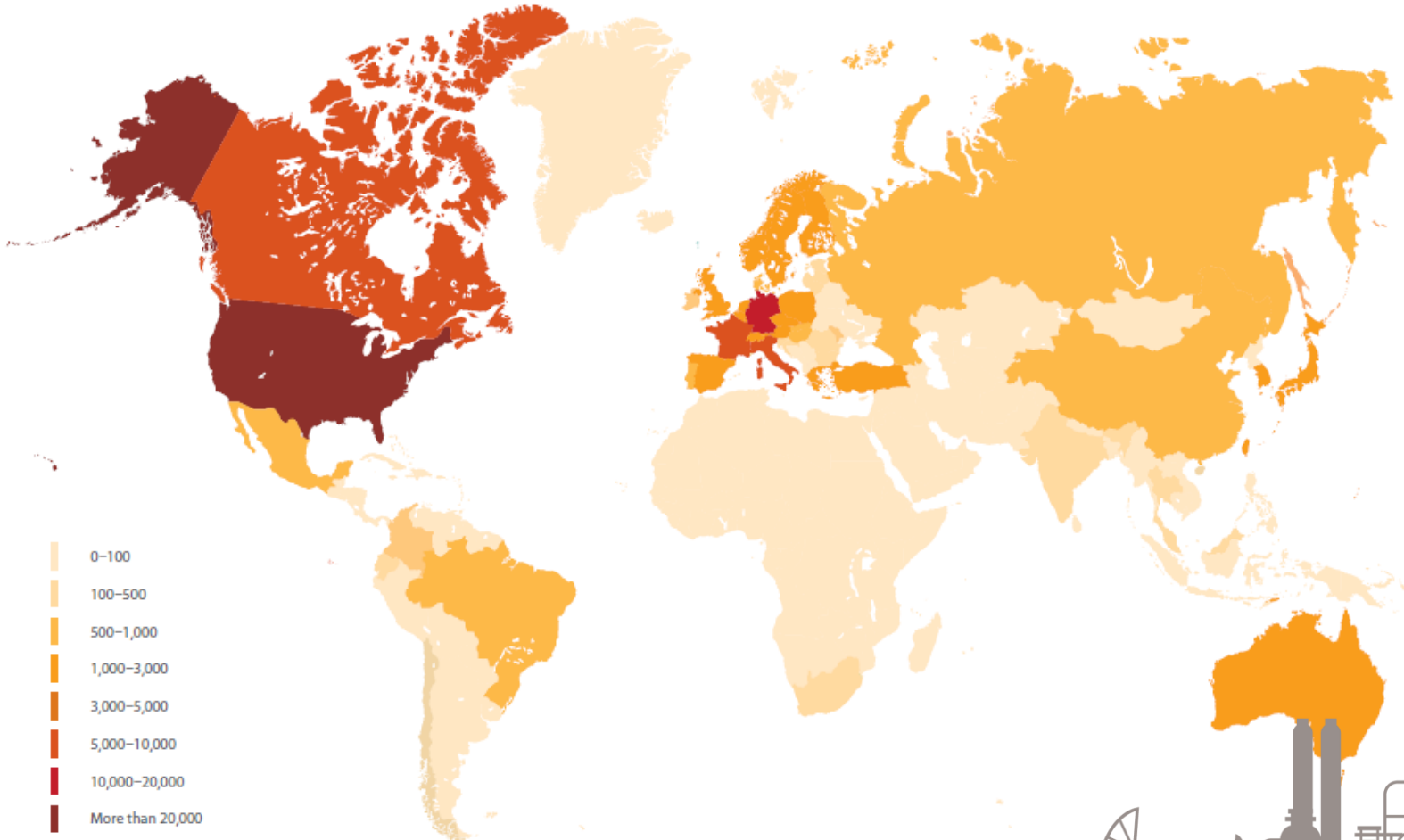
уникальная платформа объединяющая в себе множество направлений

ИНВЕНТАРИЗАЦИЯ

POSITIVE TECHNOLOGIES

Пром.системы – самые «недоступные»?

- **Более 150 000 промышленных систем оказались подключенными к Интернет**
- **Около 15 000 из них имеют критические уязвимости**



TECHNOLOGIES

https://www.ptsecurity.com/upload/ptru/analytics/ICS-Vulnerability-2016-rus.pdf

АСУ ТП: доступность через Интернет

Компонент АСУ ТП	Найденное количество
ЧМИ/SCADA + ПЛК/ТУД (RTU)	25 264
ТУД/ПЛК	18 233
Электроизмерительный прибор	17 979
ЧМИ/SCADA	13 485
Сетевое устройство	5 016
Сенсор	907

Компонент АСУ ТП	Найденное количество
Конвертер интерфейсов	408
Автоматический выключатель	361
Электронное устройство	179
Инвертор	17
РЗА	9
Другие	76 229

УЯЗВИМОСТИ

POSITIVE TECHNOLOGIES

АСУ ТП: уязвимости в цифрах

47% Высокую степень риска имеют 47% среди выявленных уязвимостей АСУ ТП

14% Лишь 14% исправлены в течение трех месяцев

1/3 Около 1/3 доступных через Интернет систем управления не защищены: лидируют системы автоматизации зданий и управления электроэнергией

MaxPatrol 8: детальный анализ уязвимостей

РЕСУРСЫ

- Настольные Приложения
- Операционные системы
- Сетевое оборудование
- СУБД
- SAP
- ВЕБ
- Виртуальные среды
- VPN
- АСУ ТП
- Антивирусы

PCI DSS, ISO 27001, Персональные данные

FORENSIC
- Поиск следов атак
- Обнаружение закладок
- Нелегитимное ПО

COMPLIANCE
- Контроль соответствия стандартам

AUDIT
- Системные проверки
- Анализ конфигураций
- Анализ ПО
- Инвентаризация

PENTEST
- Поиск уязвимостей
- Сетевое сканирование
- Аудит веб-приложений
- Сканирование СУБД

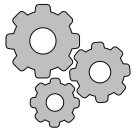
База знаний уязвимостей и ПО

Корпоративные стандарты

ОТЧЕТНОСТЬ

УПРАВЛЕНЧЕСКАЯ

АНАЛИТИЧЕСКАЯ



ТЕХНИЧЕСКАЯ

- Соответствие стандартам
- Инвентаризация активов
- Динамика изменений
- Данные по уязвимостям

НАБЛЮДАЕМОСТЬ И ИНТЕРПРЕТАЦИЯ

POSITIVE TECHNOLOGIES

События ИБ – в чём сложности?

192.168.0.23:43987→203.45.65.201:1433 SQL Injection Attack 23Mar10 1930:003 user=jones

Промышленные системы? Хотим видеть!

Исходный трафик

```
0000   23 12 14 00 0f 00 f4 01 00 fe 33 00 64 a1 2c 0c 92 05 10 f5 01 00 00 34 00 64 a1 2c 0c 92 05 10
0020   f6 01 00 07 34 00 64 a1 2c 0c 92 05 10 f7 01 00 12 06 00 64 a1 2c 0c 92 05 10 f8 01 00 15 06 00
0040   64 a1 2c 0c 92 05 10 f9 01 00 14 06 00 64 a1 2c 0c 92 05 10 fa 01 00 d2 00 00 64 a1 2c 0c 92 05
0060   10 fb 01 00 d3 00 00 64 a1 2c 0c 92 05 10 fc 01 00 d3 00 00 64 a1 2c 0c 92 05 10 fd 01 00 ff ff
0080   00 64 a1 2c 0c 92 05 10 fe 01 00 ff ff 00 64 a1 2c 0c 92 05 10 ff 01 00 ff ff 00 64 a1 2c 0c 92
00a0   05 10 00 02 00 d2 00 00 64 a1 2c 0c 92 05 10 01 02 00 d3 00 00 64 a1 2c 0c 92 05 10 02 02 00 d3
00c0   00 00 64 a1 2c 0c 92 05 10 03 02 00 e8 03 00 64 a1 2c 0c 92 05 10 04 02 00 e8 03 00 64 a1 2c 0c
```

Частичная обработка событий

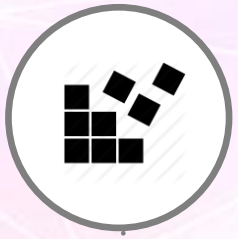
```
Протокол: IEC104, Тип информационного объекта: T1_M_SP_NA_1, причина передачи: 11,
объект информации 25 в состояние 0,
отправитель: 172.50.0.52, получатель:  172.50.0.72
```

Интеллектуальная обработка событий из трафика

```
Сообщение IEC104 от 172.50.0.52 на 172.50.0.72:
«Заземляющий нож QSG2: отключен»
```

PT ISIM™

Обнаружить злоумышленника



Регистрация цепочек атак

Атаки на бизнес логику

Журнал события безопасности

Провести расследование инцидентов

Регистрация инцидентов ИБ

Уязвимости конфигурации

Данные об активах

Защита промышленных систем: реализуема, бизнес-эффективна

Российские железные дороги повысили киберзащищенность

Александр Панасенко 06 июля 2016 - 16:20

Государство | Positive Technologies | Защита АСУ ТП | Анализ защищенности | Кибербезопасность

Компании Positive Technologies, «Бомбардье Транспортейшн (Сигнал)» и Научно-и проектно-конструкторский институт и связи на железнодорожном транспорт сообщают о разработке комплексной киберзащищенности микропроцессорн управления движением поездов.

Продукт включает в себя сенсор анал трафика на базе системы управления кибербезопасности Positive Technologi Security Incident Manager (PT ISIM), а кибербезопасного мониторинга Cyber Разработанная система — это первый промышленного внедрения подобных устройств в транспортной отрасли не только на террито мире.

Проект Positive Technologies и «Бомбардье Транспортейшн (Сигнал)» стал лучшим отраслевым решением по версии Global CIO

27 января 2017

26 января 2017 года крупнейшее сообщество IT-директоров Global CIO объявило результаты конкурса «Проект года». Проект по повышению киберзащищенности микропроцессорных систем управления движением поездов, применяемых на сети дорог ОАО «РЖД», победил в номинации «Лучшее отраслевое решение» категории «Транспорт и логистика».

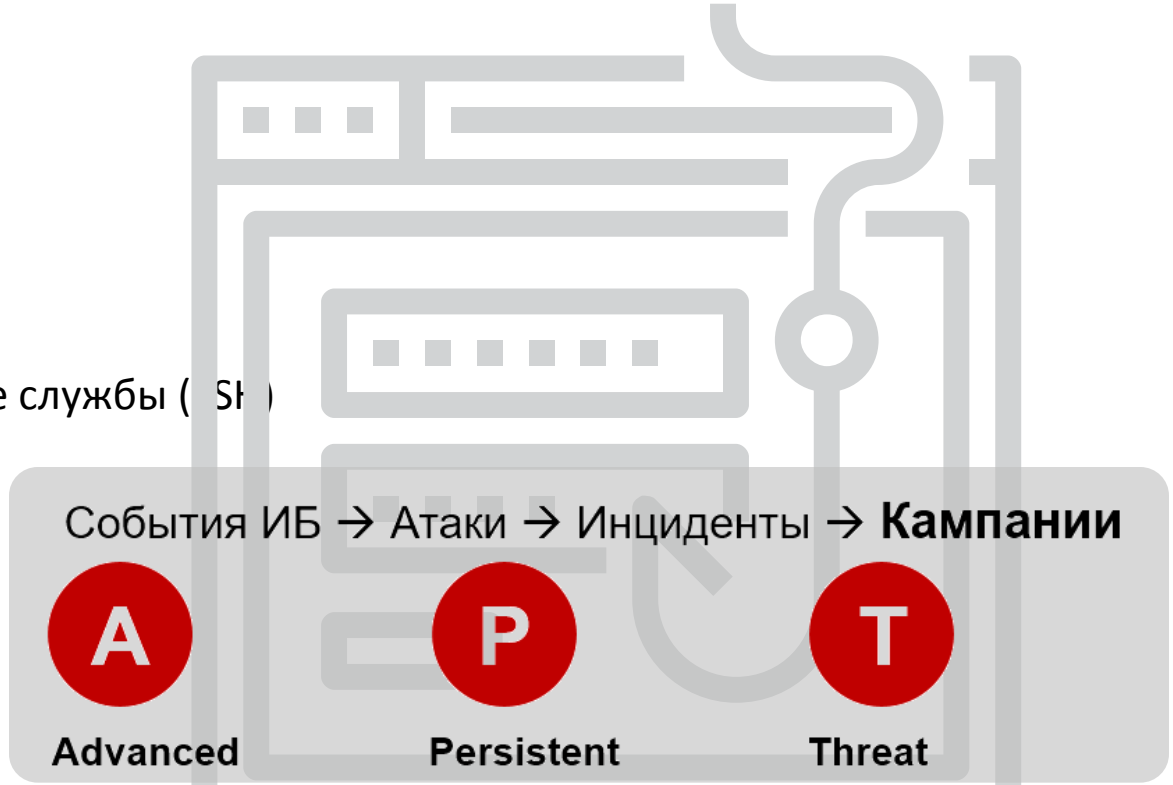
Работы были выполнены совместными усилиями специалистов ООО «Бомбардье Транспортейшн (Сигнал)», ОАО «НИИАС» и компании Positive Technologies при активной поддержке ОАО «РЖД». Была разработана комплексная система повышения киберзащищенности микропроцессорных систем управления движением поездов, включающая в себя сенсор анализа сетевого трафика на базе системы управления инцидентами кибербезопасности PT Industrial Security Incident Manager (PT ISIM) и устройство кибербезопасного мониторинга CyberSafeMon. Система стала первым в мире практическим опытом обеспечения безопасности микропроцессорных систем железнодорожной автоматики, была отмечена экспертным советом по кибербезопасности ОАО «РЖД» и получила первое место в номинации «Системы диагностики и управления» в конкурсе ОАО «РЖД» на лучшее качество подвижного состава и сложных технических систем.

ОСВЕДОМЛЕННОСТЬ ОБ УГРОЗАХ

POSITIVE TECHNOLOGIES

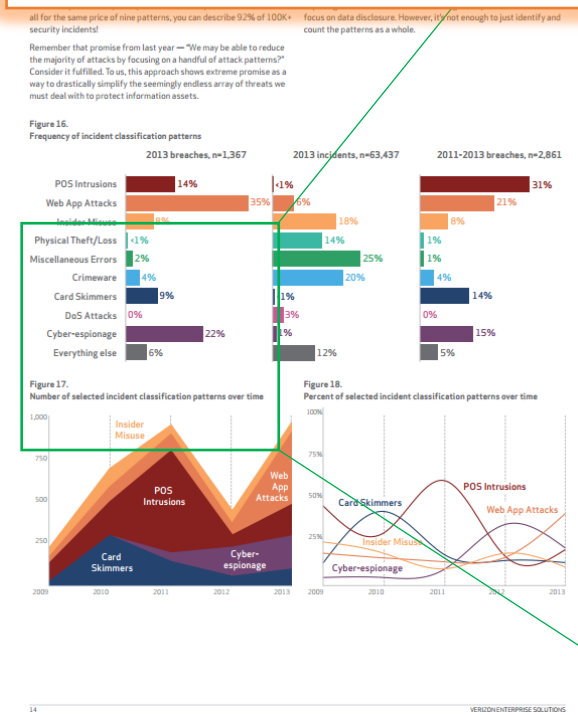
PT ESC: Экспертиза по угрозам
Типовой сценарий: ожидайте целевых атак

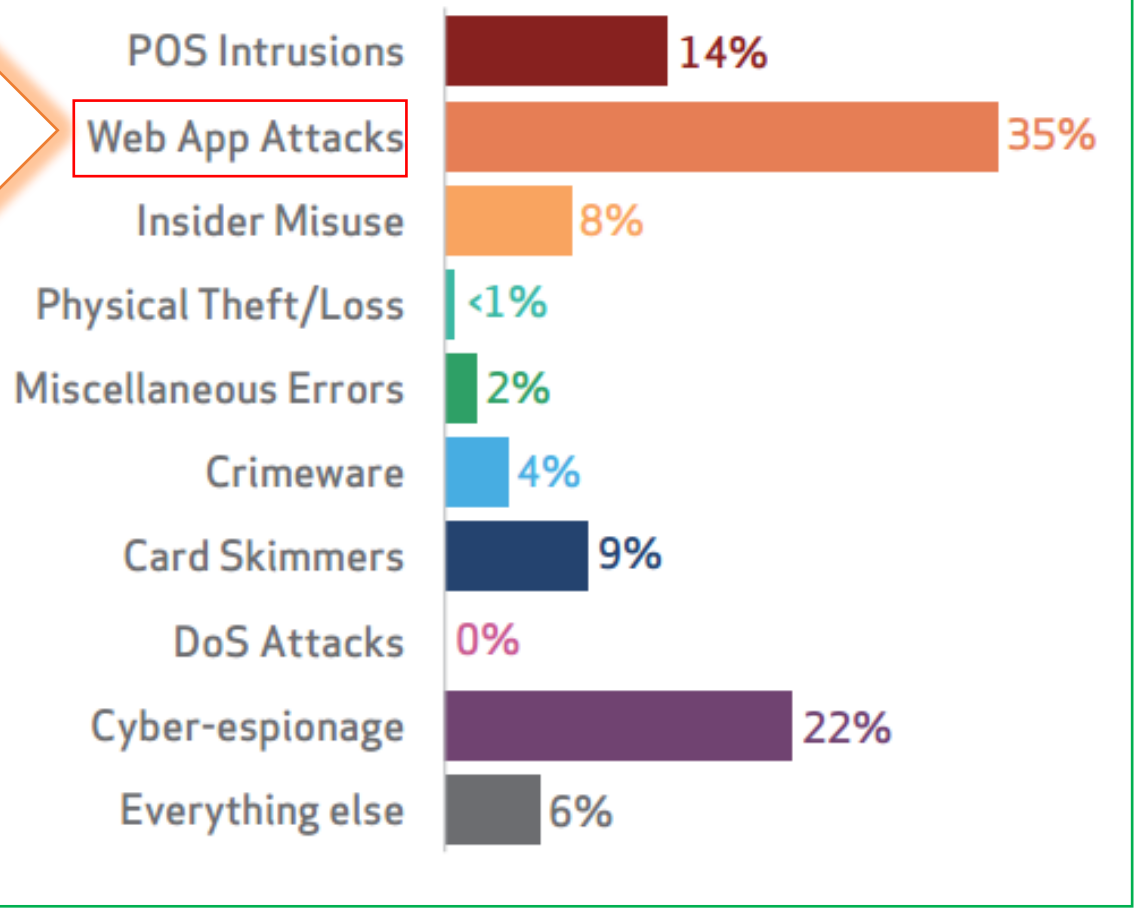
- Проникновение в систему
  - Целевой фишинг
  - Документы с вредоносным содержимым
    - Не обнаруживается антивирусом
- Закрепление в системе
  - Устранение систем защиты
  - Бэкдоры, замаскированные под легитимные сетевые службы (SH)
- Планирование реализации угрозы
  - Анализ компонентов и архитектуры системы
  - Анализ «важности» захваченной системы
- Подготовка к реализации угрозы
  - Выведение из строя средств противодействия сбоям
  - Запуск DDoS-атаки на колл-центры
- Осуществление атаки: нарушение тех.процесса
- Затруднение восстановления: удаление файлов и остановка процессов



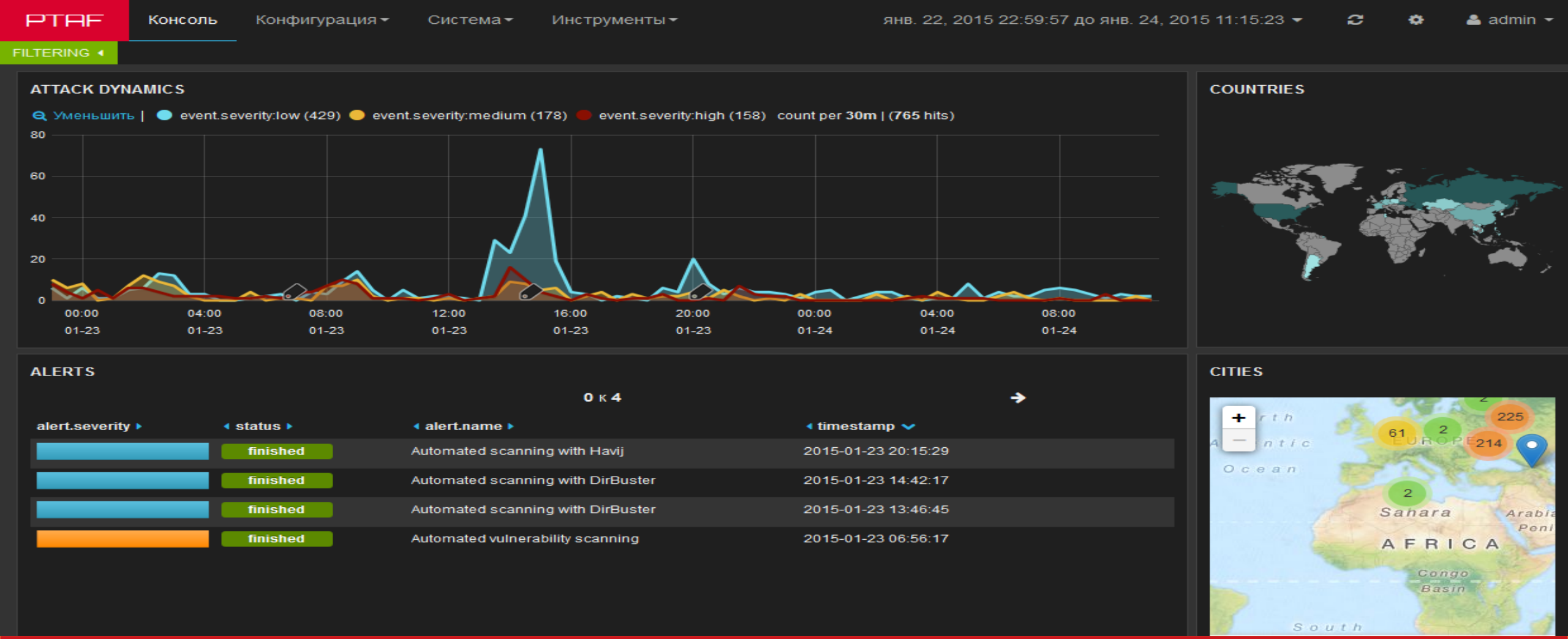
Что чаще ломают?

Статистика взломов:
35% - это веб





Verizon 2014 Data Breach Investigations Report



PT Application Firewall

СПЕЦИФИКА ОБЛАСТИ

POSITIVE TECHNOLOGIES

«Позитивный» подход: учесть все источники событий

Поддержка источников

– 100 –

– 200 –

– 400 –

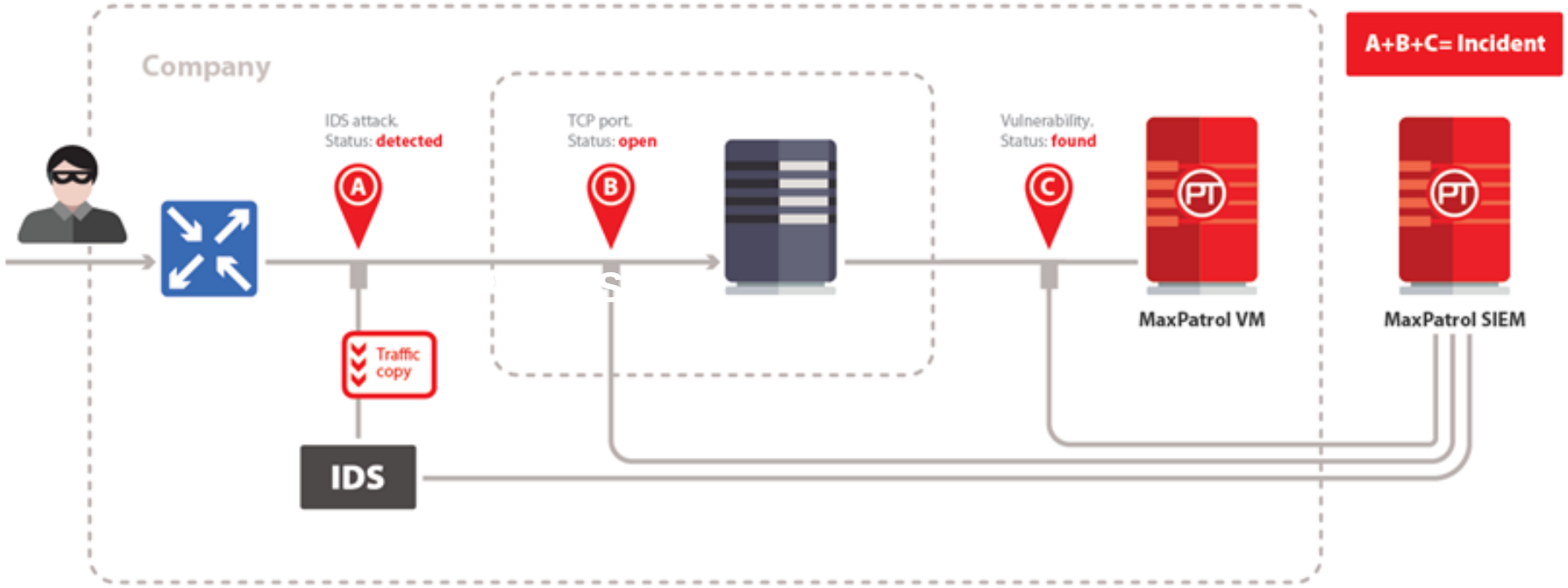
MaxPatrol SIEM: от типовых к специфическим угрозам

Корреляции на основе модели инфраструктуры и расширяемая база правил

Полная модель инфраструктуры

Платформа MaxPatrol

База знаний PTKB



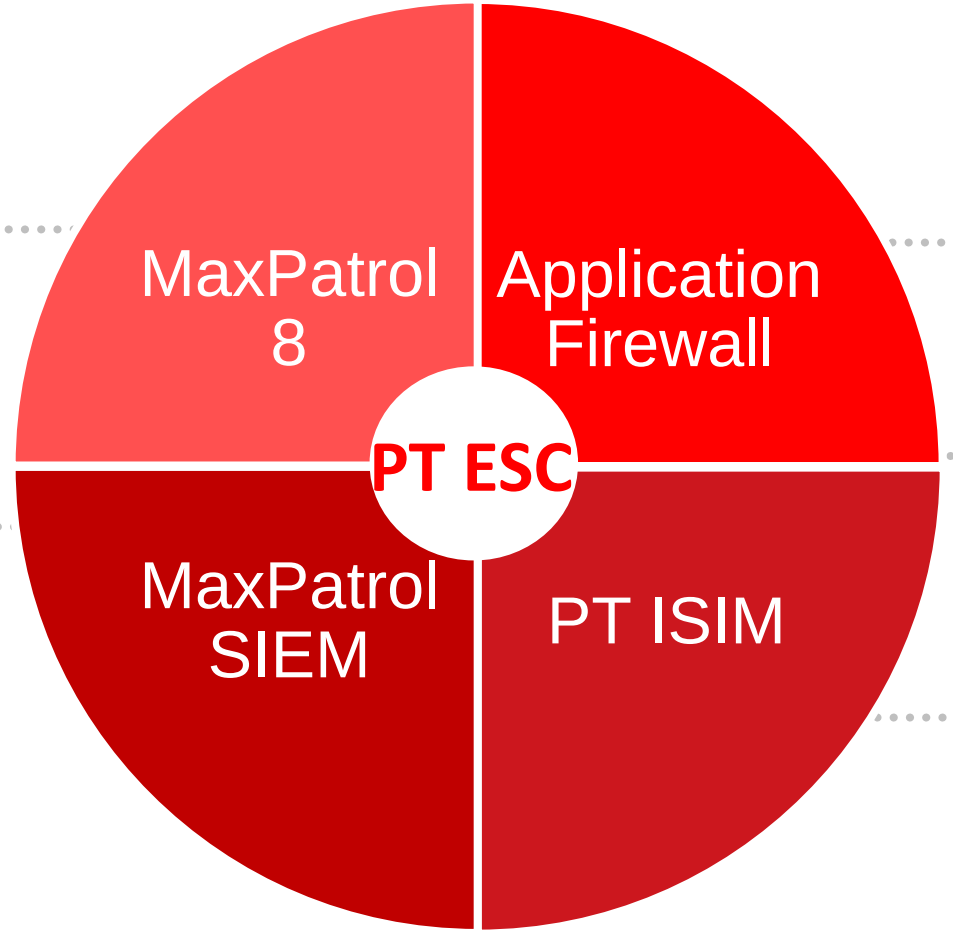
ДИНАМИКА И ИНТЕГРАЦИЯ КОНТРОЛЕЙ

POSITIVE TECHNOLOGIES

Интеграция контролей ИБ: промышленные системы

Инвентаризация и контроль уязвимостей

Контроль ИТ событий, действий пользователей и изменений в системе



Защита приложений

Анализ защищенности и расследование инцидентов (сервисы)

Контроль событий АСУ ТП

Безопасность это ~~купите наш продукт~~ процесс (и люди)

Но для организации процесса нужны:

- Наблюдаемость
  - Интерпретируемость
- Интеграция ИБ ИТ и ОТ
- …

Table 1.Roles matrix for incident response and analysis in control systems[14].

Incident Response Activity	Incident Handling Team	IR Coordinator (with CS)	Primary Security (POC)	Incident Response Director	CS Incident Manager	CS Security Specialist	CS Engineering Support	(CS Vendor Coordinator)
Detection								
Detection	P	S	P					
Initial Reporting and Documentation	P	P	P					
Response Initiation								
Incident Classification	P		P	S	P			
Escalation			P	P	P	S		
Emergency Action	P		P	P		S	S	P
Incident Response/ Evidence Collection								
Mobilization	S	P	S	P	P	S	S	S
Investigation	S	P	P	S	P	P	S	S
Containment	P	P	S	S	P	P	P	S
Incident Recovery/Evidence Analysis								
Recovery Planning		S	S	S	P	P	P	S/P
Restoration		S	S	S	P	P	P	S
System Upgrade		S	S	S	P	P	P	S
Incident Closure/ Process Reporting								
Summary Report		P	S	S	S	P	S	
Mitigations/ Reporting			P	P	P	P	S	S
System Upgrade	P		P	P	P	P	S	

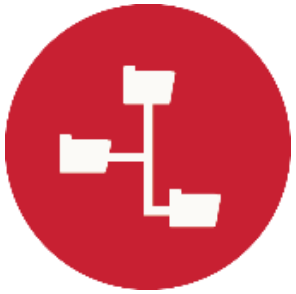
Illustrated above as P are primary activities; and S – secondary functions

http://www.osce.org/

Фокус на автоматизацию

Уведомления

Инциденты



Многоуровневые и распределённые корреляции

Ретроспективный анализ

Сбор данных

Мониторинг

Технологическое «Ядро»

- Наблюдаемость
  - Активов, их свойств
  - Событий, изменений
- Управление
  - Выявление инцидентов
  - Отслеживание
- Интеграция
  - Систем безопасности
  - Изменений в организации
- Процессы
  - Коммуникации
  - Оптимизация и развитие

Путь к Безопасности

1. Наши продукты, наши **компетенции**
   https://www.ptsecurity.com
2. Анализ уязвимостей и/или пилот,
   мониторинг событий ИБ
   pt@ptsecurity.com
3. Решение актуальных ИБ-задач
   - Инфраструктура: Maxpatrol & Maxpatrol SIEM
   - AppSec: PT AF & AI
   - Индустриальная безопасность: PT ISIM
4. Осведомленность об угрозах и методах атак
   - PHDays
   - SecurityLab.ru
   - PT Research

POSITIVE TECHNOLOGIES

Positive Research 2017

https://www.ptsecurity.com/

http://securitylab.ru

PHDays 7 – 23-24 мая

PHDays.com

phd7

Positive Hack Days

THE STANDOFF

23-24 Мая 2017

ENEMY INSIDE

Компетенции, реализованные в продуктах и сервисах

MaxPatrol **MaxPatrol** SIEM	Мониторинг безопасности на всех уровнях информационной системы, а также сбор событий и анализ состояния системы
PT Multiscanner	Выявление вредоносных файлов, полученных по почте и хранящихся в корпоративных базах, десятками антивирусов
Сервисы	**Тест на проникновение** **Анализ защищенности** **Анализ угроз и расследование инцидентов**
PT Application Inspector **PT** Application Firewall	Защита веб-порталов и бизнес-приложений на этапе разработки и эксплуатации
PT ISIM **PT** SS7 Attack Discovery	Выявление атак на критически важные системы телекомов и промышленных предприятий