Необходимость и достаточность решений и сервисов ИБ для эффективного расследования инцидентов

POSITIVE TECHNOLOGIES

Качалин А.И.

Positive Technologies: Expert Security Center

+ Исследование уязвимостей и анализ защищенности
+ Мониторинг безопасности и реагирование на угрозы
+ Анализ и расследование инцидентов
+ Технологические исследования и консалтинг ИБ

Безопасность приложений

- Минимальные требования по ИБ
- Детальность и форматы логирования
- Требования к компонентам
- Требования к платформам инфраструктуре
- Требования к процедурам сопровождения
- Доступность исходных кодов

Общие требования по ИБ

- Унифицированные пункты ТЗ
- Автоматизированные проверки соответствия
- Проверка изменений

Ситуация:
1 департамент ИБ должен обеспечить ИБ:

- 200 приложений (веб, мобильные)
- Разные модели угроз
  - Платежные ПО
  - Медицина
  - …
- 20 подрядчиков
- 10 внутренних функциональных заказчиков
- 5 площадок размещения
- …

Что делать когда уже всё запущено и «запущено»?

Уязвимость алгоритмов защиты и их реализации

- Уязвимость серверной части
  - 54% уязвимы для XSS
  - 71% используют 2ФА
    - 46% возможна кража у банка или у клиента
    - 25% возможен перехват 2ФА
- Атака на клиентов (2ФА)
    - 90% SIM клонируется
    - В 75% возможен перехват

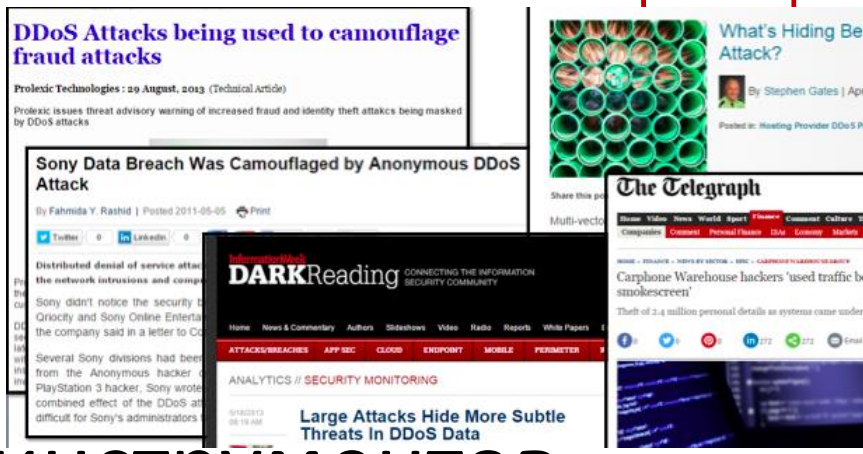
- Пятница 19.02 10:30 #ibbank 2016. Тимур Юнусов: «СМС – «золотой» стандарт двухфакторной аутентификации»
- Новая статистика Positive Research 2015 – в марте
  - 54% некорректная реализация 2ФА, возможность обхода

«Инцидент»: необходимо, но недостаточно

Атака → Инцидент → **Кампания**

- Долгосрочные «проекты» атакующих
  - Вектор по объекту
  - Вектор по технологии
- Комплексные атаки, составляющие инцидент
- Кампании (Adversary Campaign)
  - Целевые
  - Массовые
  - Комбинированные (массово-целевые)

Комплексные сценарии атакующего



- DDoS SmokeScreen
- Waterholing
- Malware “Lifecycle”
- Эволюция тактики и инструментов
  - RAT=LAT+легитимные методы доступа
  - Защита RAT от обнаружения и исследования
  - Эффективность Соц. Инженерии >100%

Продукты и решения ИБ

Взгляд вендора:

- Эффективные механизмы сбора и структуризации данных
- Возможности машинного обучения
- Знания экспертов
- Информации об угрозах (Threat Intel)
- Фильтрация и приоритезация информации
- Комбинация методов

- Инвентаризация, анализ уязвимостей, менеджмент инцидентов
  - **((Xspider))**
  - **((MaxPatrol 8))**
  - **((MaxPatrol SIEM))**
- Анализ трафика, анализ ПО
  - **((PT NAD))** – Анализ сетевого трафика
  - **((PT AF))** – Application Firewall
  - **((PT AI))** – Application Inspector
- Продвинутые средства противодействия новым угрозам
  - **((PT Multiscanner))**
  - **((PT Honeypot))**

POSITIVE TECHNOLOGIES

Эффективные ИБ-решения: реализация экспертных сценариев

Продвинутые сервисы обнаружения угроз PT MultiScanner + Honeypot

Ловушка (Honeypot)
Эмуляция уязвимых сервисов
Отправка на анализ файлов в песочницу

Пассивный и активный сбор артефактов
Пассивный анализ передаваемых в трафике файлов, веб-ссылок с возможностью уведомления
Активный контроль передачи опасных объектов в трафике «на лету»
Анализ почтового, веб трафика, поддержка протокола ICAP

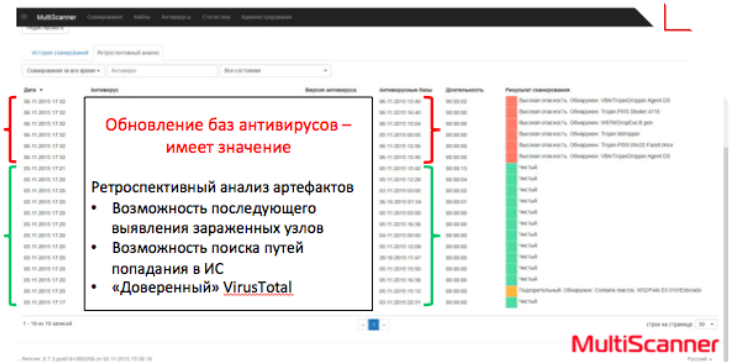
Статический и динамический анализ
Файлов, веб-сайтов на наличие зловредного поведения
Собственная среда исполнения
Поведенческий анализ ПО
Статический анализ на множественных движках AB
Black/white/репутационные списки

Песочница (Sandbox/Detonation Chamber)
Защищенная изолированная среда исполнения ПО
Контролируемое окружение
Защита от детектирования

Индикаторы компрометации

POSITIVE TECHNOLOGIES ptsecurity.com

Multiscanner: ретроспективный анализ



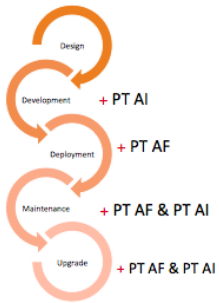
Обновление баз антивирусов – имеет значение

Ретроспективный анализ артефактов
- Возможность последующего выявления зараженных узлов
- Возможность поиска путей попадания в ИС
- «Доверенный» VirusTotal

MultiScanner

ptsecurity.com

Сервис защиты веб-сервиса при помощи PT AF/AI



+ PT Application Inspector – анализатор исходных кодов

+ PT Application Firewall – решение для защиты корпоративных приложений

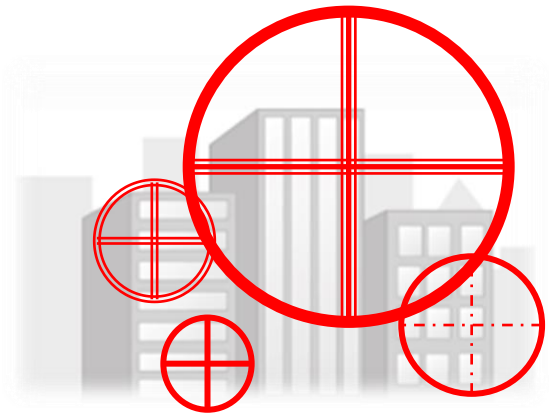
+ **Генерация экспресс-патчей для PT AF по результатам анализа PT AI**

POSITIVE TECHNOLOGIES ptsecurity.com

Network Attack Discovery: расследование

POSITIVE TECHNOLOGIES ptsecurity.com

Совокупность угроз, или «а завтра они проснулись»



- Ежедневные атаки
  - Вирусы в сети/в почте
  - Соц. Инженерия (почта, веб)
  - Атаки на веб-ресурсы
- Инциденты
  - Заражение файлового сервера шифровальщиком
  - Заражение сервера печати – утечка информации
- Кампании
  - APT-1 (предположительно Китай) – 9 мес.
  - APT-2 (предположительно США) – 1,5 года
  - APT-3 – признаки возможности доступа, несколькими способами

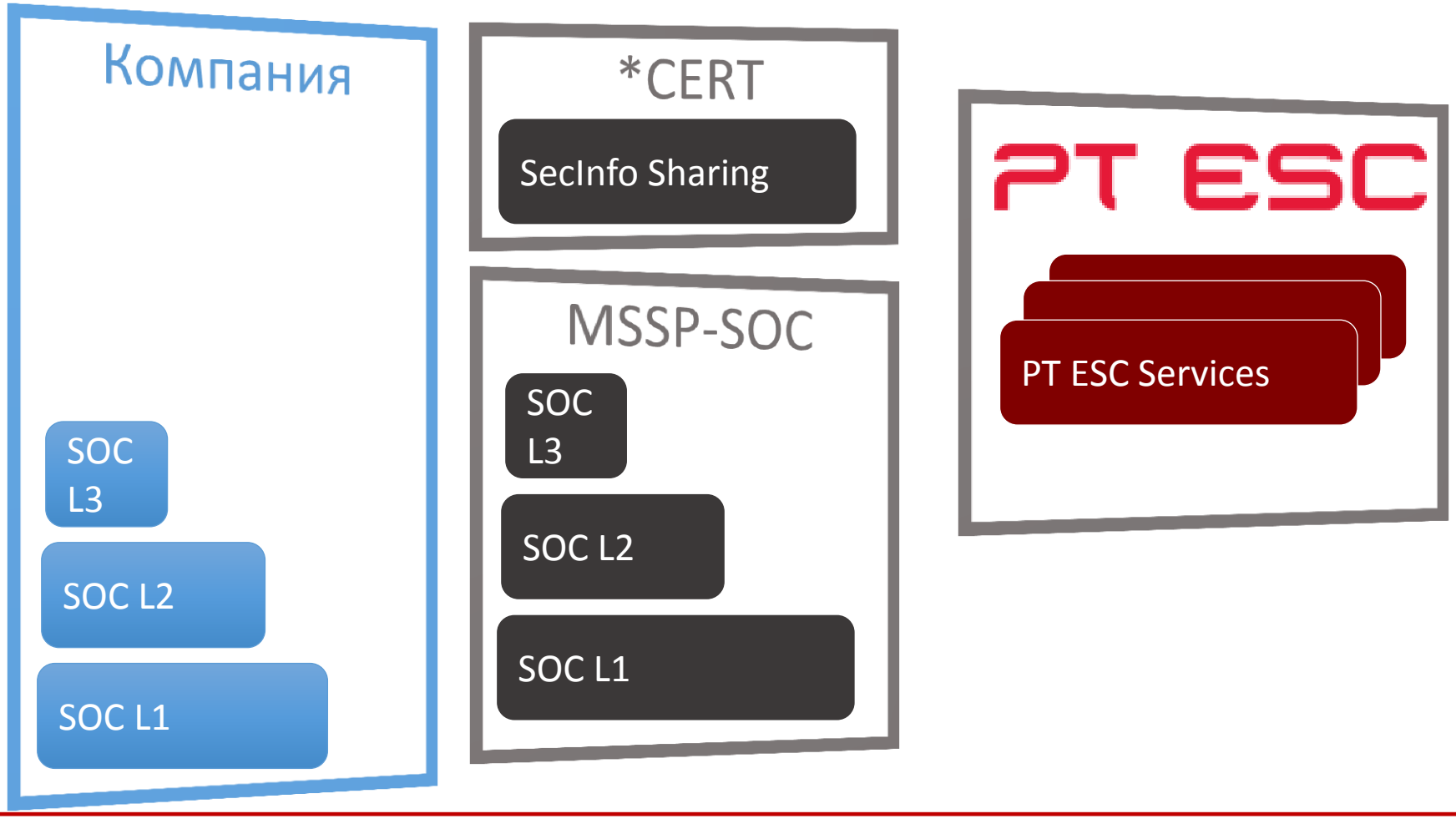
Задачи OpSec/SOC – что сделать?

- Работа в реальном времени
  - Телефонный информационный центр
  - Мониторинг и ранжирование событий
- Сбор информации и отслеживание тенденций
  - Создание службы кибераналитики
  - Распространение данных службы кибераналитики
  - Объединение служб кибераналитики
  - Отслеживание тенденций
  - Оценка угроз
- Анализ инцидентов и реагирование
  - Анализ инцидентов
  - Наблюдение за инцидентами, сбор информации
  - Координация реагирования на инциденты
  - Применение мер противодействия
  - Применение мер противодействия во внешних инф.системах
  - Удаленные работы по противодействию
- Расследование инцидентов
  - Выявление и анализ скрытых уязвимостей
  - Ретроспективный анализ инцидентов
- Обеспечение ЖЦ технических средств и методическое сопровождение
  - Настройка и эксплуатация средств защиты
  - Настройка и эксплуатация средств мониторинга
  - Обслуживание сенсоров
  - Создание сигнатур и правил
  - Разработка и поддержка методик и инструкций
- Аудит и противодействие внутренним угрозам
- Оценка и повышение уровня защищённости
  - Инвентаризация
  - Поиск и оценка уязвимостей
  - Тестирование на проникновение
  - Оценка ИБ используемого ПО
  - Консультации по ИБ
  - Тренинги по ИБ, повышение осведомленности
  - Оповещение по актуальным угрозам
  - Распространение информации о тактике атакующих
  - Публикация информация, работа со СМИ

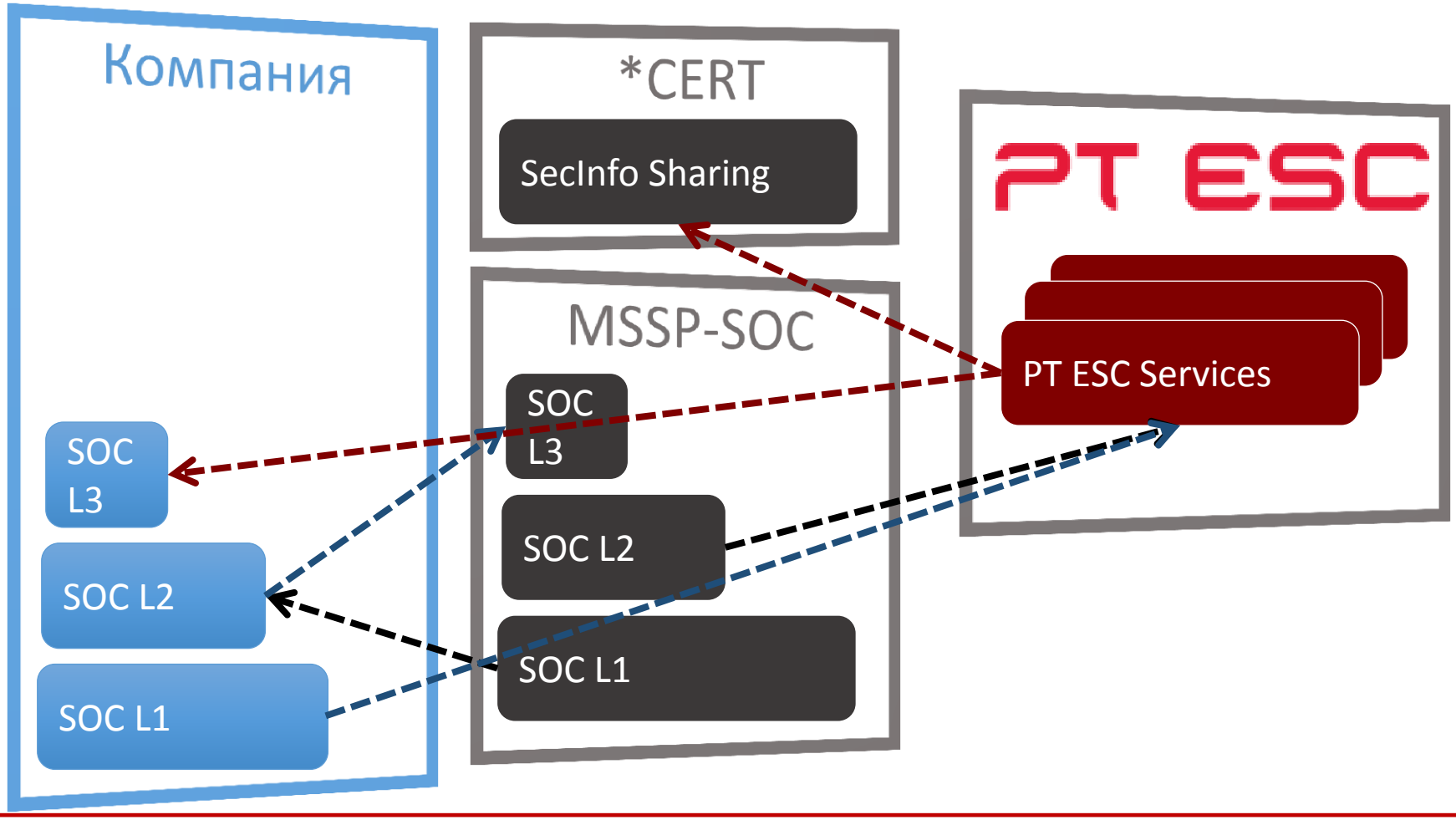
В каком объеме решать задачу?

- Архитектура SOC?
  - Централизованный
  - Распределенный
- Какие функции реализованы?
  - Кому делегировать оставшиеся?
- Покрытие по времени
- «Производительность» и качество
  - Время реакции
  - Период проведения мероприятий
  - Полнота/глубина анализа

Операционная безопасность: внутренние и внешние сервисы

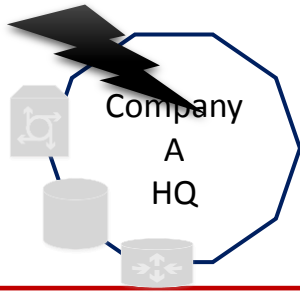


Операционная безопасность: внутренние и внешние сервисы



Защита периметра – ~~не~~актуально?!

- **40%** сервисов на периметре более **были уязвимы** в течение 1 года
- **50%** вероятность эксплуатации критической уязвимости в течение 1 месяца с момента публикации
- **80%** уязвимостей на периметре старше 1 года
- **80%** внешний атакующий может получить доступ к внутренней сети в случаев (без применения методов СИ)
- **75%** случаев: атакующему не требуется высокого уровня квалификации для проведения успешных атак
- **55%** полный контроль над системой после «пробива» периметра



По материалам мониторинга PT ESC за 2015 год, Verizon

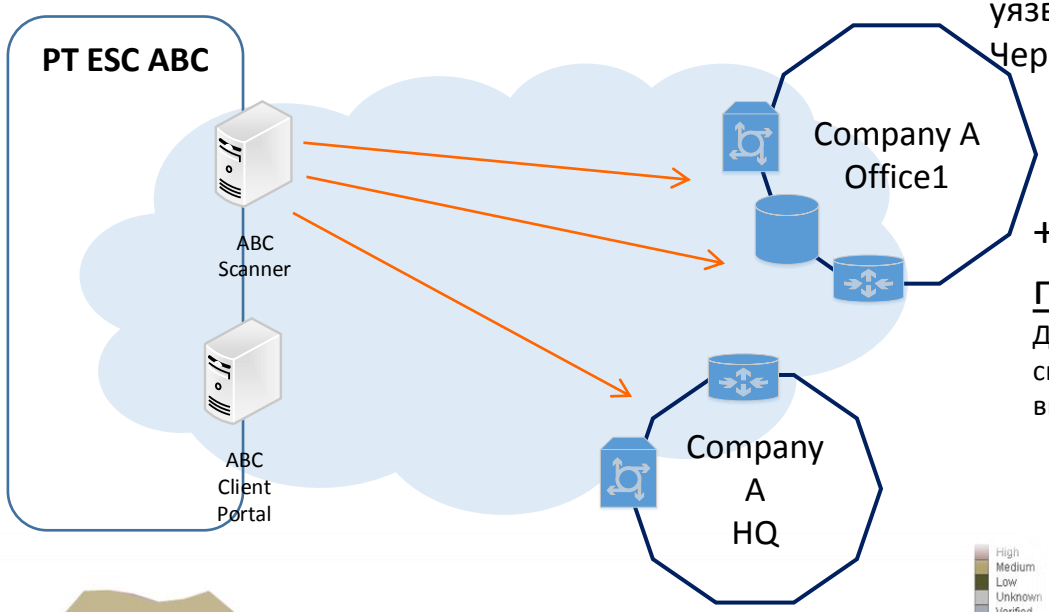
Более 10 организаций, 130 тысяч ip, 15 тысяч уязвимостей

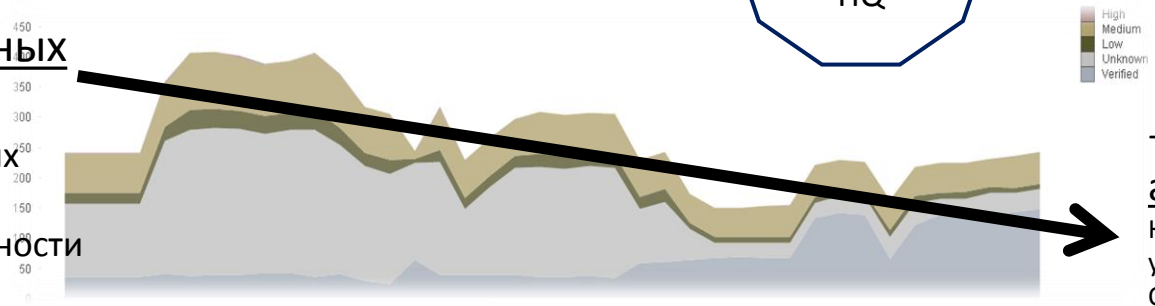
PT ESC ABC – контроль безопасности периметра – автоматизированный **экспертный** сервис

+ Актуальная информация об угрозах
База PTKB

+ Контроль процесса сканирования
До сети класса B за 1 день

+ Аналитика и выявление критичных уязвимостей
Контроль нежелательных сервисов
Оценка с учетом критичности ресурсов





+ Инвентаризация
Узлы, сервисы, версии, уязвимости
Черные/белые списки

+ Клиентский портал и отчеты
Доступ к результатам сканирования в удобном виде

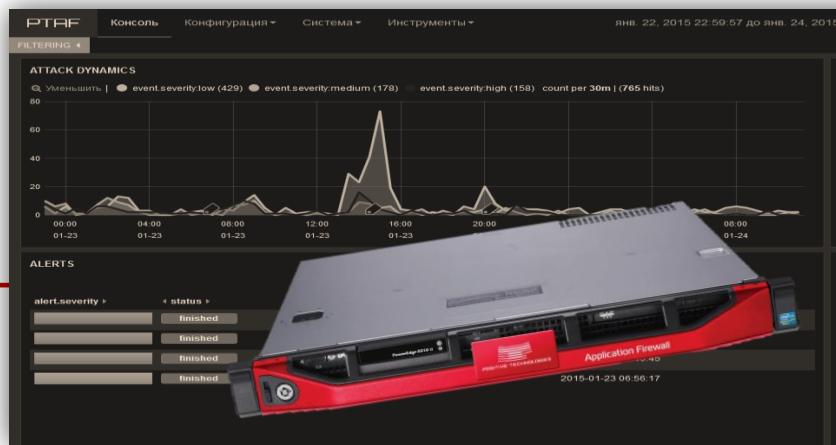
+ Единый инструмент
Для больших сетей и распределенных организаций

+ Стратегическая аналитика
Контроль эффективности устранения уязвимостей
Окно уязвимости

Мониторинг безопасности и защита Веб-сервиса: Экспертиза + передовые технологии PT AF

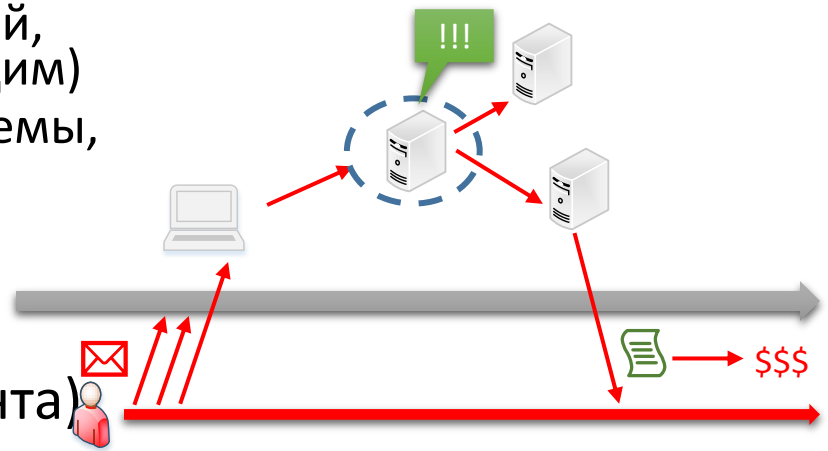
- Веб-сервисы критичны
  - Доступ к хранимой информации
  - Точка «входа» во внутреннюю сеть
  - Лицо организации
- Высокая динамика
  - Обновление сервиса - ежедневно
  - Появление новых угроз
  - Самый атакуемый тип сервиса
- Экспертиза и большой объем работы
  - Много «шума»
  - Исследователи «вебщики»
- Выявление инцидента
  - Взаимосвязь Веб и ИТ – комплексная задача
  - Большой объем логов для обработки

- Мониторинг безопасности
  - Оперативное оповещение о критических срабатываниях
  - Актуальная информация о новых угрозах и уязвимостях
- Периодические проверки
  - Сводный анализ атак на ресурс
  - Выявление аномалий, рекомендации по расследованию
- Экспертные возможности
  - Анализ границ инцидентов (цепочки атак)
  - Верификация уязвимостей (проверка эксплойтов)
- PT AF как инструмент форензики



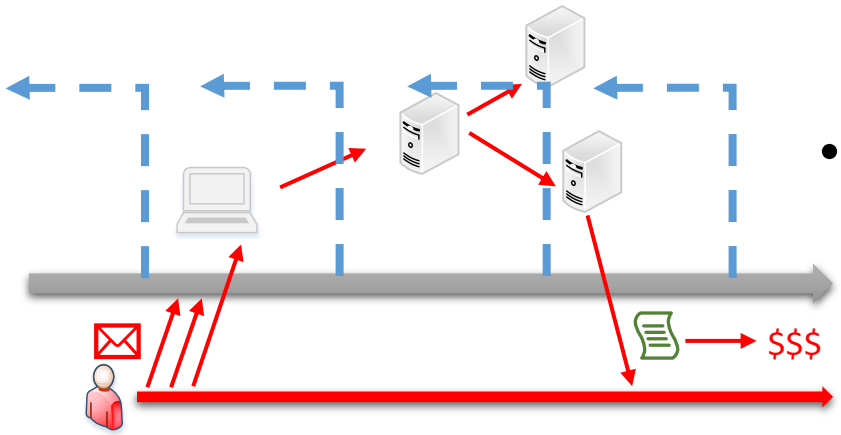
Анализ и Расследование инцидентов

- Анализ инцидента
  - Выявление связанных событий безопасностей и их анализ
  - Анализ атак (совокупности событий, результатов, достигнутых атакующим)
  - Фиксация границ инцидента (системы, время)
  - АЗ по инциденту и первичные рекомендации
- Расследование инцидента (по результатам Анализа инцидента)
  - Исследование артефактов инцидента
  - Анализ средств и тактики атакующег
  - Атрибуция атакующего (категория нарушителя, конечные цели)
  - Прогноз возможностей атакующего
  - Рекомендации



Расследование инцидентов: Корректно диагностировать и **бороться с причинами и последствиями**, а не симптомами

Ретроспективный анализ: выявление инцидентов



Проверить подозрения, выявить упущенные инциденты: **возможно ещё не поздно минимизировать ущерб**?!

- Оценка готовности
- Периодические проверки
  - Ежеквартально
  - По критическим системам
  - По подозрениям на инциденты
- Поиск следов компрометации
  - Анализ событий безопасности
  - Сбор и первичный анализ артефактов
  - Анализ журналов. Backward Anomaly Rollout
  - Отложенный автоматизированный анализ потенциально-вредоносного ПО
  - Отчет - сводка попыток компрометации и событий безопасности

PT ESC: экспертные сервисы

Внешние угрозы ИТ-инфраструктуре

Усиленный контроль периметра (ABC)

Внешнее тестирование на проникновение

Мониторинг угроз сетевого трафика

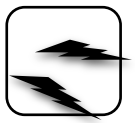
Анализ инцидентов ИБ

Защита от угроз Веб-сервисов

Анализа защищенности Веб-сервисов (black/grey/whitebox)

Мониторинг безопасности и защита Веб-сервисов

Анализ инцидентов в Веб-сервисах



Защита от внутренних угроз

Внутренне тестирование на проникновение

Анализ инцидентов

Анализ готовности к реагированию и расследованию инцидентов

Анализ эффективности центров мониторинга ИБ

Экспертные сервисы ИБ

Ретроспективный анализ и выявлении инцидентов

Реагирование на инциденты

Расследование инцидентов

Профильные отраслевые сервисы

PT ESC

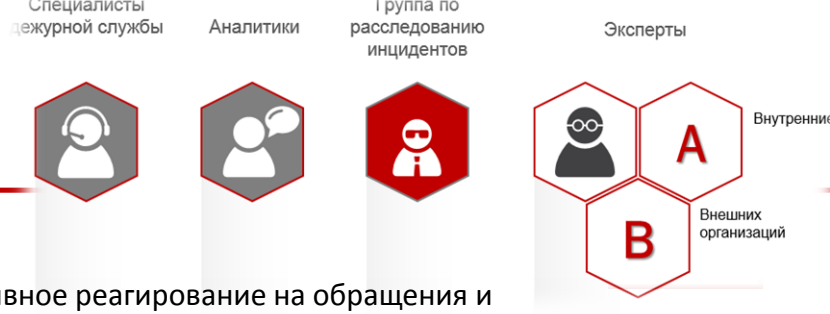
Спасибо за внимание!

Алексей Качалин akachalin@ptsecurity.com

POSITIVE TECHNOLOGIES

ptsecurity.com

PT ESC



- **Команда PT ESC.** Команда экспертного центра обеспечивает оперативное реагирование на обращения и собираемую информацию, работает с инцидентами и координирует взаимодействие с командой PT, партнерами, производителями и сообществом.
- **Команда экспертов PT.** Исследовательский центр Positive Technologies насчитывает более 150 человек и является одним из крупнейших в Европе. Специалисты центра заслужили репутацию экспертов мирового уровня по защите важнейших современных отраслей — веб-порталов и онлайн-банков, АСУ ТП и ERP, сетей мобильной связи и облачных технологий.
- **Взаимодействие с партнерами и производителями средств ИБ –**возможности компании PT в рамках технологического партнерства получения комментариев и содействия со стороны ключевых производителей, интеграторов, эксплуатирующих организаций информации позволяет оперативно исключать ложные срабатывания систем обеспечения, сузить область анализа инцидента, а также существенно масштабировать объем оказываемых услуг PT ESC.
- **Взаимодействие с ИБ-сообществом.** Компания PT активно участвует и развивает ИБ сообщество, являясь организатором конференции PHDays.
- **Специализированные методики инструменты и сервисы.** Команда PT ESC непрерывно развивает компетенции по ключевым областям специализации в ходе выполнения работ. Существенная доля этих знаний становится доступна потребителям в виде обновлений сигнатур, правил и эвристик для продуктов PT.
- **База знаний уязвимостей и угроз,** используемая в PT ESC, — одна из крупнейших в мире. Эксперты Positive Technologies обнаружили и помогли устранять множество уязвимостей в продуктах таких компаний, как Cisco, Google, Microsoft, Oracle, SAP, Siemens, Huawei, Schneider Electric, Honeywell. База постоянно пополняется за счёт новых исследований и аналитических сервисов.
- **Сервис PT ESC – сделано для Вас!** Обеспечение ИБ – это непрерывный процесс. В рамках наших услуг мы непрерывно отслеживаем состояние зафиксированных обращений и открытых инцидентов. Мы предлагаем гибкие возможности подключения систем сбора информации, различные варианты обращений для получения сервиса и возможность интеграции с вашими системами отслеживания задач.

Исследовательский центр Positive

+ Одна из самых больших научно-исследовательских лабораторий по безопасности в Европе
+ 100+ обнаружений 0-day уязвимостей в год
+ 150+ обнаружений 0-day уязвимостей в SCADA
+ 30+ обнаружений 0-day уязвимостей в Telco
+ Наши знания использ[illegible] лючевые промышленные цент[illegible]

Web Application Security Consortium

C|EH Certified Ethical Hacker

Center for Internet Security

Google Microsoft cisco ORACLE SAP vmware SIEMENS