ВЕБИНАР: ПРАКТИЧЕСКИЕ ОСОБЕННОСТИ ВНЕДРЕНИЯ СИСТЕМ КЛАССА DLP

Роман Ванерке
Руководитель отдела технических решений
АО «ДиалогНаука»

10 мая 2016, всех с праздником!

ДиалогНаука

Содержание

- Цели и задачи, которые заказчик обычно ставит перед DLP, его ожидания
- Часто допускаемые ошибки
- Цели проекта по внедрению DLP
- Этапы проекта по внедрению DLP
- Преимущества и недостатки
- Общее описание Forcepoint TRITON APX
- Выводы
- Ответы на вопросы

Цели, задачи и ожидания Заказчика

- Основная цель – защититься от утечек или контролировать действия сотрудников

- Задачи
  - установить систему DLP
  - контролировать все документы по всем каналам
  - архивировать все – потом найду, что нужно

- Ожидания – утечки сократятся в разы!

Какие ошибки при этом допускаются?

- Не определяется:
  - что необходимо защищать (какие есть типы информации, примеры этих документов)
  - где хранятся документы
  - как эти документы появляются, куда передаются, как обрабатываются (бизнес-процессы)

- Документы, как правило, хранятся скопом на файловом хранилище – вот вам учетка, снимите отпечатки
- Отсутствие политики хранения конфиденциальных документов (хранятся где как, без аудита доступа)
- Или еще лучше – вот примеры документов, давайте определим ключевые слова и настроим политики на них

- Применение только системы DLP, забывая, что это один из элементов системы защиты от утечек

Цели проекта по внедрению DLP

- Минимизировать риск утечки конфиденциальной информации
- Соответствие требованиям:
  - ПДн,
  - PCI DSS,
  - ISO2700x,
  - Соглашения с партнёрами и т.п.
- Повышение эффективности бизнеса
- Уменьшения стоимости продуктов и услуг

- Аудит
- Контроль электронной переписки, веб-трафика и работы на АРМ
- Внедрение системы
- Сокращение времени расследования инцидентов

Этапы проекта

- Идентификация и классификация ИОД, определение собственников информации, мест хранения, бизнес-процессы
- Приоритезация ИОД по степени риска, требованиям аудита и регуляторов
- Определение политик хранения, обработки и передачи, как часть общего подхода к защите ИОД
- Выбор и развертывание системы защиты от утечек
- Разработка документации, обучение сотрудников
- Превентивное автоматическое реагирование
- Регулярный контроль и оценка эффективности

Преимущества и недостатки

- Преимущества:
  - Всесторонний охват – все типы информации, каналы передачи данных
  - Встраивание системы DLP в бизнес-процессы компании, не нарушая их, там где допускается передача конфиденциальных данных
  - Минимизация рисков утечки конфиденциальной информации

- Недостатки:
  - Требуется время на проведение подготовительных работ – аудит и анализ рисков
  - Не всегда в штате компании есть квалифицированные специалисты, способные выполнить эти работы
  - Требуется либо нанимать высококвалифицированных специалистов, либо привлекать внешнего подрядчика - деньги

Архитектура TRITON

AP-WEB	AP-EMAIL	AP-DATA
✓ Advanced Threats	✓ Spear-Phishing	✓ Content Aware DLP
✓ Data Theft & Loss	✓ URL Sandboxing	✓ Data Discovery
✓ Threat Dashboard	✓ Advanced Threats	✓ DLP Gateway
✓ Malware Sandbox	✓ Data Theft & Loss	✓ DLP Endpoint
✓ Forensic Reports	✓ Anti-Spam	✓ MacOS & Windows
✓ Forensic Data	✓ TLS Encryption	✓ Off-Network Prot.
✓ SSL Inspection	✓ Advanced Encrypt.	✓ Portable Decrypt.
✓ Social Media	✓ Cloud Archiving	✓ 1,700+ Policy/Temp.
✓ App Controls	✓ Image Analysis	✓ Drip DLP Detect.
✓ Video Controls	✓ Cloud Cleansing	✓ OCR of Image Text
✓ Hybrid Solution	✓ Hybrid Solution	✓ Geo-Location

Преимущества

FORCEPOINT AP-WEB

Контроль использования ресурсов сети Интернет и сетевых протоколов, защита от веб-угроз в реальном времени

ДиалОгНаука

Анализ в реальном времени

Forcepoint ACE

- **Механизмы анализа угроз в реальном времени**
  - Безопасность, данные, контент
  - Более 10000 различных классификаторов
- **Три движка Anti-Malware**
  - Коммерческий AV
  - Эвристический анализ
  - Вредоносные PDF
- **Защита от фишинга, репутационный анализ, анализ ссылок**
- **Composite Scoring Model**
- **Behavioral Analytics**

Примеры классификаторов ACE

- Advanced Malware Payloads ←
- Potentially Exploited Documents ←
- Mobile Malware ←
- Criminal Encrypted Uploads →
- Files Containing Passwords →
- Advanced Malware Command & Control →
- Unauthorized Mobile Marketplaces →
- OCR (Optical Character Recognition) →
- «Капельный» DLP →
- Geo-Location →

Анализ входящего трафика

Анализ исходящего трафика

Анализ исходящего трафика в части утечек

Real Time Security Scanner

- Определение вредоносного кода в коде веб-страниц (Flash, Silverlight, другие)
- RTSS анализирует веб-страницу в режиме реального времени
- Оценка уровня угрозы
- ACE использует различные технологии одновременно: RTSS для URL, репутацию, RTCC, сигнатуры и другие для выявление 0-day угроз!

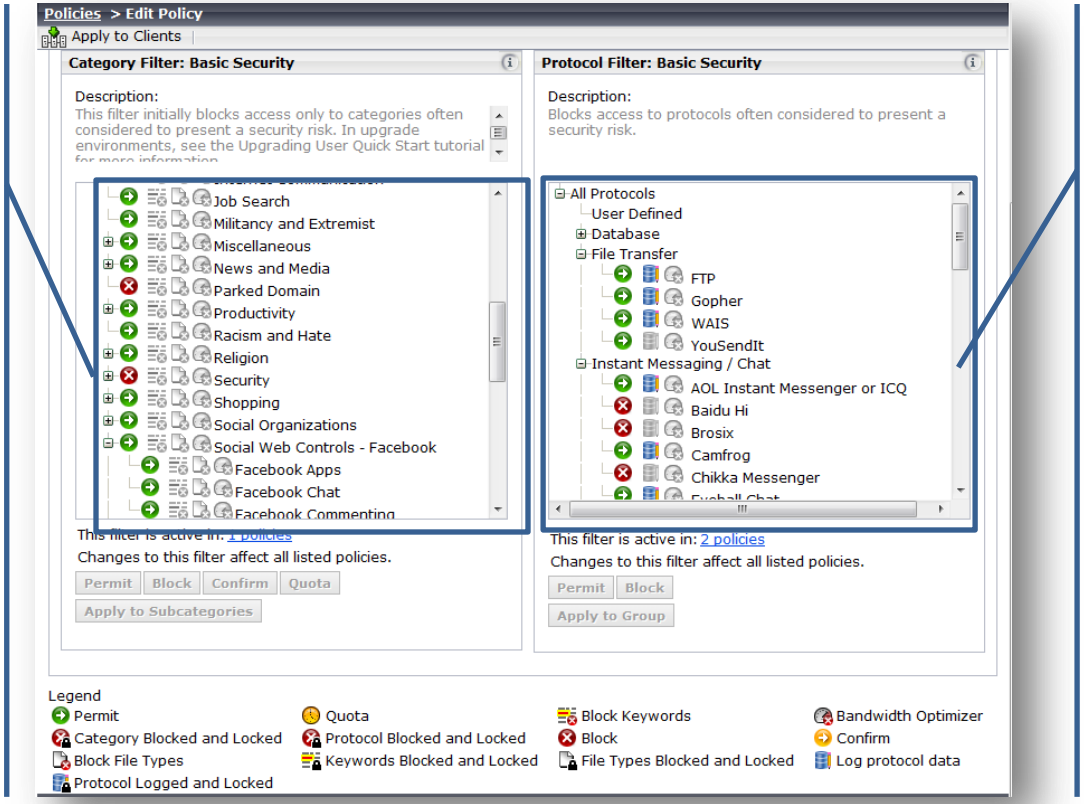
Real Time Content Classification (RTCC)

Это все сайты, отнесенные к категории «Социальные сети»?

Forcepoint анализирует реальную информацию (контент) на странице и проводит классификацию внутри категории «Социальные сети»

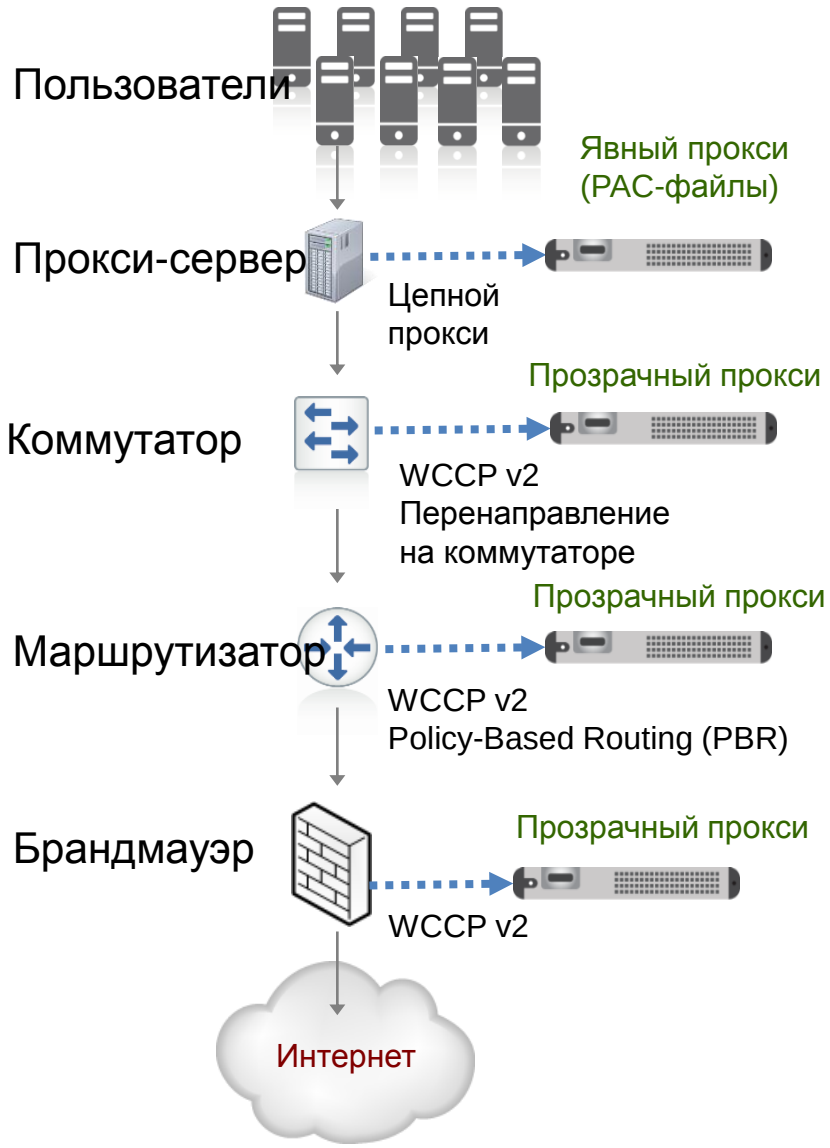
Тонкая настройка политик

- Более 120 различных категорий
- Тонкое управление доступом к социальным сетям
- Простое создание политик



- Более 100 различных приложений
- Включая управление видео
- Инспекция SSL

Варианты развертывания



Явный прокси-сервера

- Хорош для заказчиков, использующих GPO, SMS или WPAD-файл
- Не затрагивает сетевую инфраструктуру

Цепочка прокси-серверов

- Трафик направляется с имеющегося прокси-сервера
- Не затрагивает пользователей

Прозрачный прокси-сервера

- Трафик направляется с коммутатора, маршрутизатора или брандмауэра
- Не затрагивает пользователей

FORCEPOINT AP-DATA

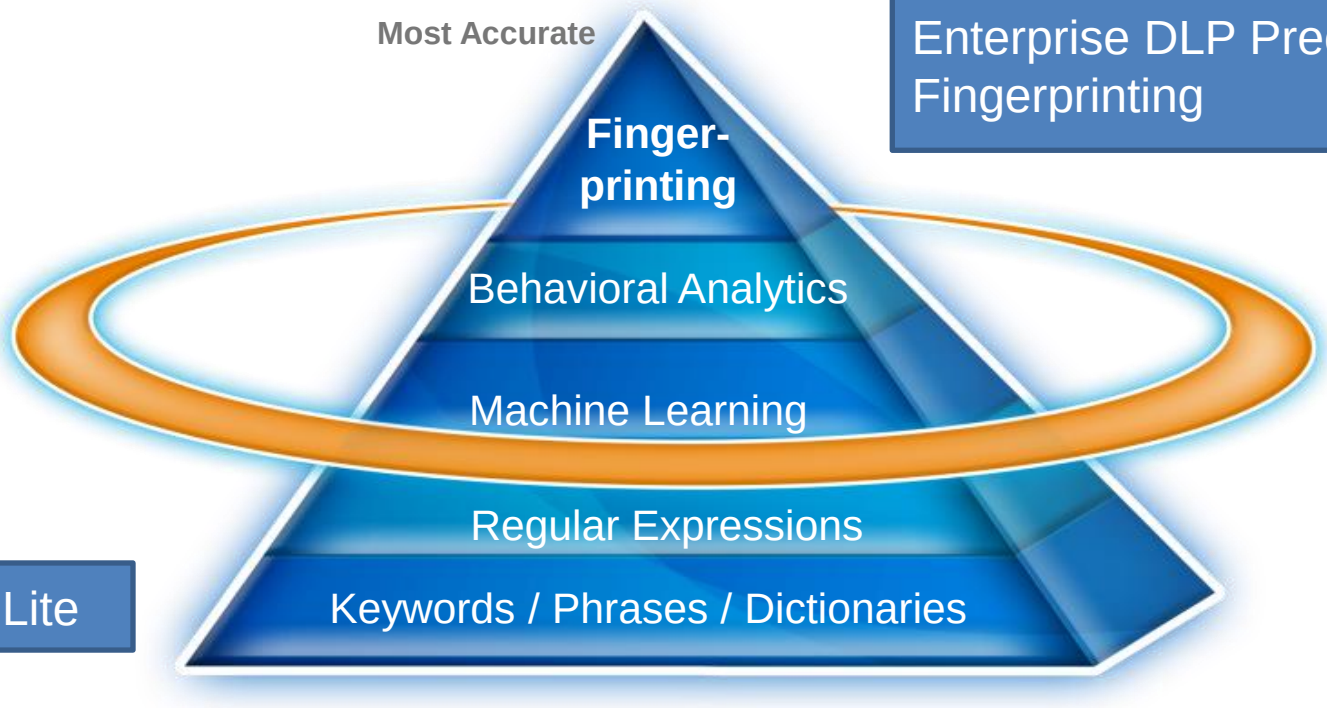
ДиалогНаука

Forcepoint AP-DATA

AP-WEB	AP-EMAIL	AP-DATA
The **most effective** anti-malware protection from **advanced threats** and **data theft**.	The **most advanced** email defenses against **blended** and **targeted attacks**.	✓ Content Aware DLP ✓ Data Discovery ✓ DLP Gateway ✓ DLP Endpoint ✓ MacOS & Windows ✓ Off-Network Prot. ✓ Portable Decrypt. ✓ 1,700 Policy/Temp. ✓ Drip DLP Detect. ✓ OCR of Image Text ✓ Geo-Location

Технология выявления утечек

- Кирпичик для создания политики
- Классификаторы определяют данные для защиты
- Высокая точность



Enterprise DLP PreciseID Fingerprinting

Базовые DLP Lite

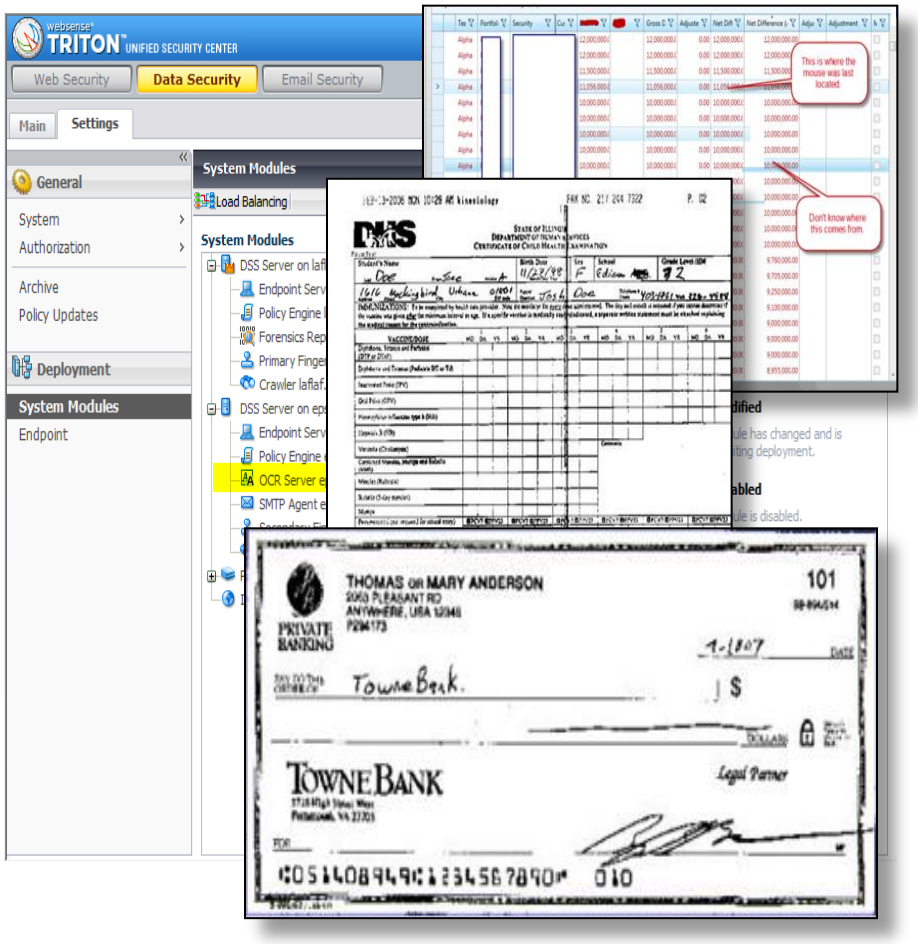
Цифровые отпечатки

- Цифровые отпечатки:
  - Баз данных
  - Сетевых каталогов
  - SharePoint \ Lotus Domino
  - другие

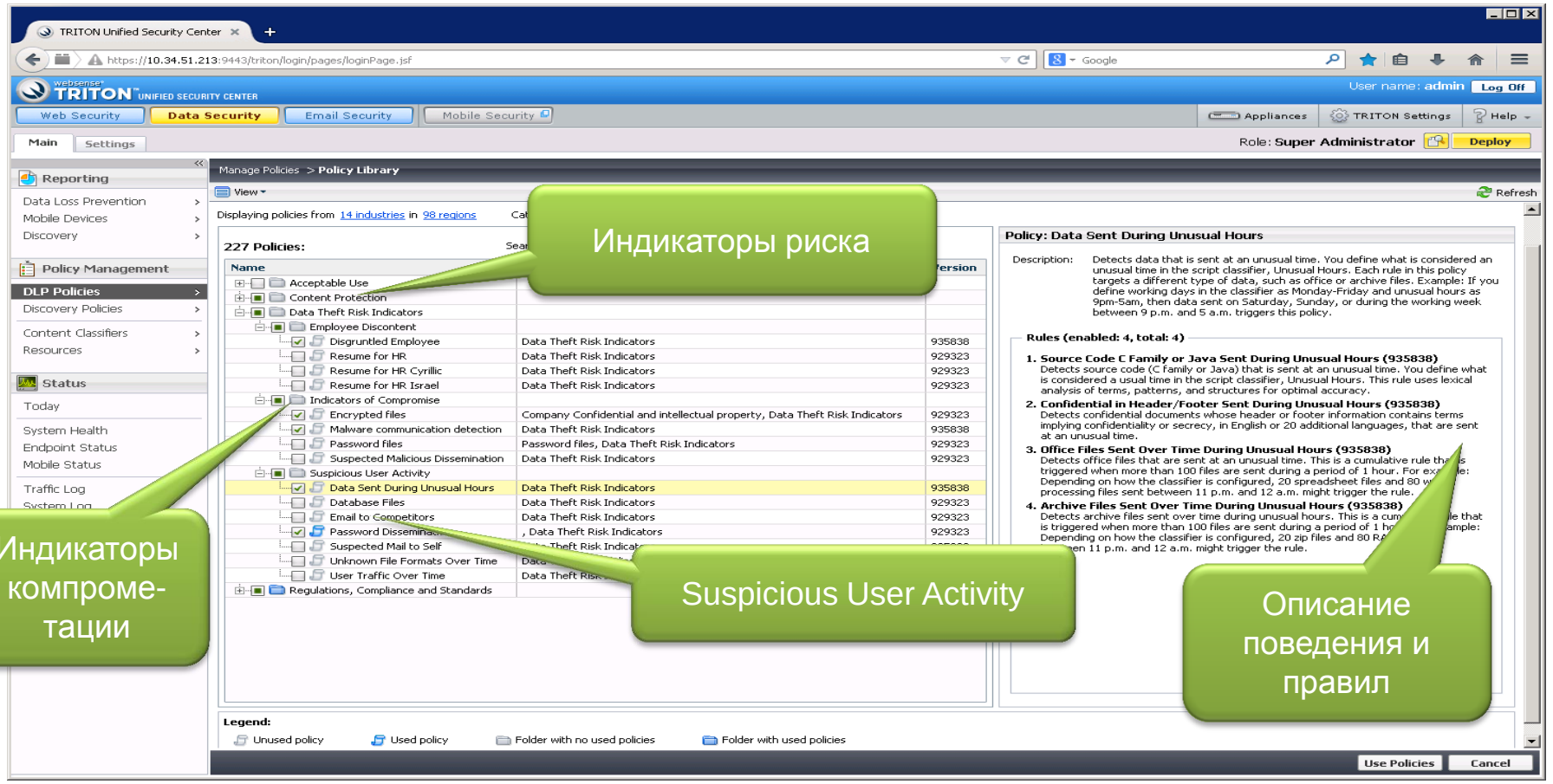
- Подключение к базе данных через ODBC
- Снятие цифровых отпечатков непосредственно с БД
- Данные не покидают БД
- Инкрементальные обновления базы отпечатков при росте исходной базы

Распознавание текста OCR)

- Используется механизмы оптического распознавания
- Определение данных в изображениях
  - Скриншоты
  - Отсканированные документы
  - Факс
  - и т.п.
- Доступен для выявления утечек через веб, почты и в рамках поиска документов по сети



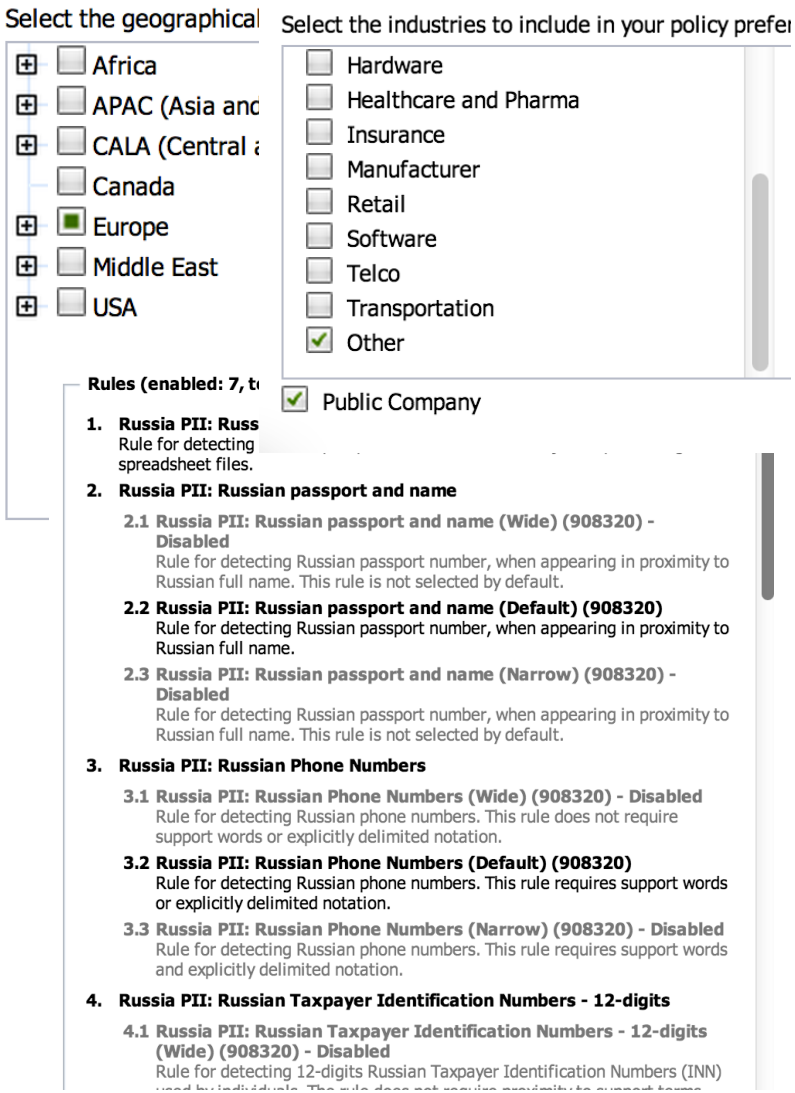
Анализ поведения



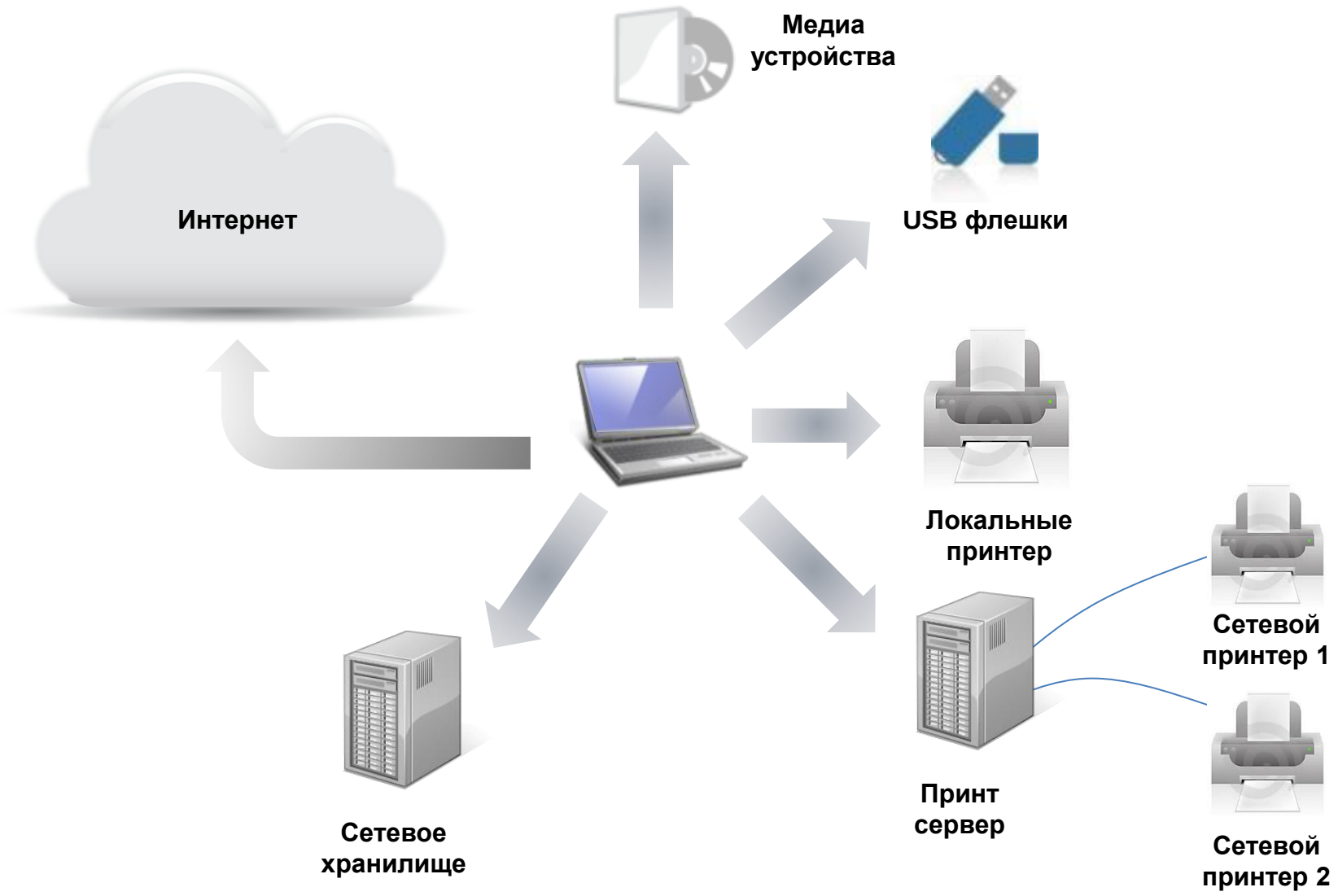
Готовые политики

- Различные классификаторы
  - Регулярные выражения, ключевые слова, словари
- Более 1700 готовых политик «из коробки», в том числе для РФ
- Удобный мастер настройки политик
- Определяет типы данных

  например: ПДн, PCI



Агент AP-Endpoint DLP



Полнота информации по инцидентам

Security Alert A

Данные:	PCI & PII
Источник	10.14.222.21
Канал:	Web
Получатель:	93.10.219.62

Security Alert B

Данные:	PCI & PII, customer database
Источник:	Joe User x1234, juser@company.com Title: Associate Dept: Finance Manager: Jane Manager x1234, jmanager@company.com
Канал:	Web
Получатель:	mail.google.com Type: Personal webmail site Location: Mountain View, CA

Подход к анализу

Ключевые клиенты Forcepoint в РФ

Финансовый сектор

ВТБ
УРАЛСИБ
Ренессанс Капитал
Кредит ЕвропаБанк
Банк Союз
Банк Интеза
БТА Банк
ОТП Банк
Доверяя друг другу
Финансовая корпорация Открытие

Промышленность

ЛУКОЙЛ
Нефтяная компания
Газпром
Газпром нефть
Enel ОГК-5
Норильский никель
Северсталь
Российская Сталь
СИБУР
«Сахалин Энерджи»
Быть ведущим источником энергии для Азиатско-Тихоокеанского региона

Телекоммуникации

МТС
COMSTAR
МТТ

Выводы

- Комплексный подход к построению системы защиты
  - Более 90% утечек, согласно отчету Verizon, можно было предотвратить используя достаточно дешевые средства и способы защиты
- Руководство компании:
  - Минимизация финансовых потерь, репутационных рисков
  - Контроль нецелевого использования ресурсов Компании
- Отдел ИБ:
  - Предотвращение и расследование инцидентов, связанных с утечкой конфиденциальной информации
- Отдел HR:
  - Выявление неблагонадёжных сотрудников. Лояльность персонала
- Отдел ИТ:
  - Снижение нагрузки на сотрудников ИТ, привлекающихся к расследованию инцидентов

Вопросы?

Роман Ванерке

117105, г. Москва, ул. Нагатинская, д. 1, стр.1

Телефон: +7 (495) 980-67-76, ext.162
Факс: +7 (495) 980-67-75

http://www.DialogNauka.ru
e-mail: rv@DialogNauka.ru