POSITIVE TECHNOLOGIES

Отчеты MaxPatrol в формате XML

Павел Лысов
старший программист
ЗАО «Positive Technologies»

Александр Веретенников
консультант
ЗАО «Positive Technologies»

Вебинары Positive Technologies: образовательная программа «Практическая безопасность»

POSITIVE TECHNOLOGIES

Часть 1.
Введение

Александр Веретенников

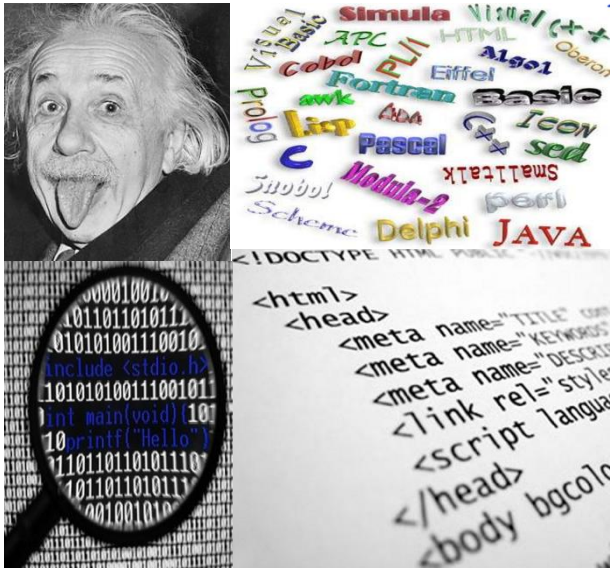
консультант

ЗАО «Positive Technologies»

POSITIVE TECHNOLOGIES

Такие разные … «языки»

Albert Einstein versus ГОСТ Р 52292-2004



Язык разметки XML: общая информация

Текст (для собственных нужд)

Пишу КАК
сЧитаю НУЖНЫМ
!

Текст (для публикации)

Записывать текст по установленным правилам, с заданным оформлением!

Ректор НОУ ВПС

МЕЖДУНАРОДНАЯ СИСТЕМА ФИНАНСОВОГО МОНИТОРИНГА

Аннотация. Сегодня можно констатировать, что в мире создана весьма надежная и эффективная организационно-правовая конструкция противодействия легализации преступных доходов и финансированию терроризма. Эта конструкция направлена на оказание помощи финансовым

Название раздела [Arial шрифт 9, полужирный, по левому краю]
Текст статьи [Arial шрифт 9, по ширине]
В случае если статья разбита на разделы, текст, включенный в разделы или подразделы, должен начинаться с новой строки после названия раздела или подраздела. Выравнивание текста по ширине страницы. Нумерация подразделов производится вручную арабскими цифрами. Новые абзацы без отступа с новой строки.

Приложение 1

Платформа 1

Приложение K

Платформа N

POSITIVE TECHNOLOGIES

Mr.XML, who are you?

POSITIVE TECHNOLOGIES

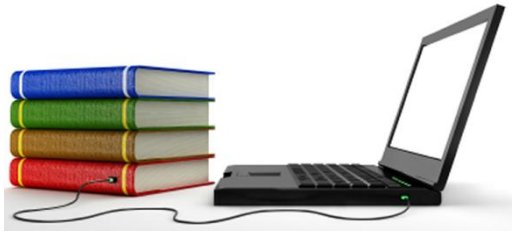
XML: ОСОБЕННОСТИ

- средство описания грамматики других языков
- средство контроля за правильностью составления документов
- универсальный способ хранения данных
- универсальный язык запросов к хранилищам информации
- средство контроля за корректностью данных, хранящихся в документах
- средство проверки иерархических соотношений внутри документа
- средство определения единого стандарта на структуру документов, содержимым которых могут быть самые различные данные
- возрастающая поддержка XML в различном программном обеспечении разных производителей (в перспективе – основной язык обмена информацией в информационных системах)

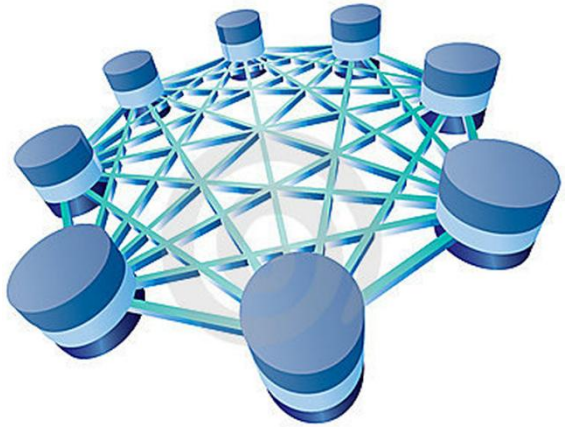
POSITIVE TECHNOLOGIES

XML : ДОБРО ПОЖАЛОВАТЬ!

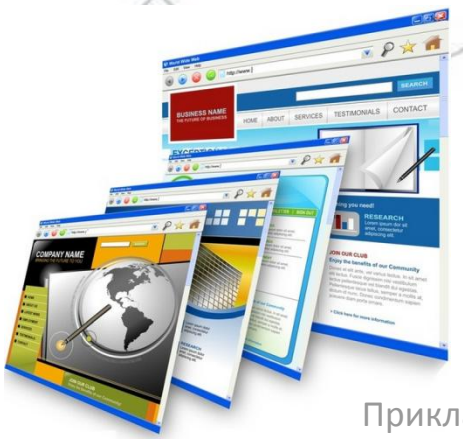
Офисные приложения (Microsoft Office)



Издательские системы (Quark Publishing System)



СУБД (Oracle Berkeley DB XML)



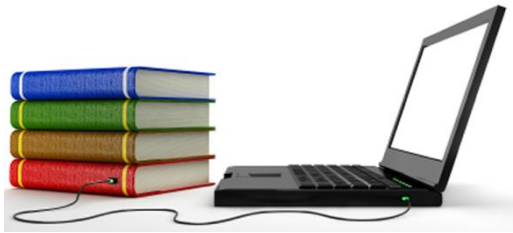
Прикладное ПО (LMS, сервисные утилиты и пр.)

Сервера управления контентом (MarkLogic Server)

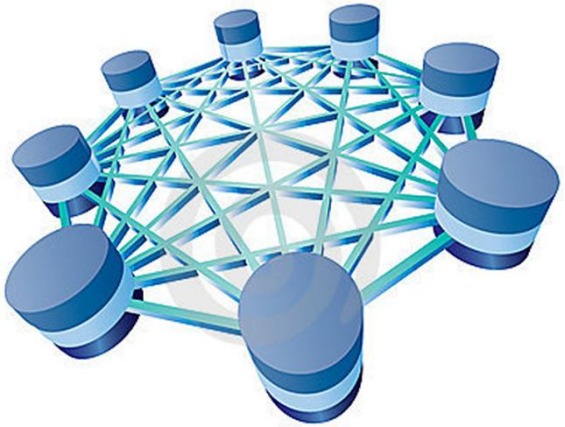
POSITIVE TECHNOLOGIES

MAXPATROL
VULNERABILITY AND COMPLIANCE MANAGEMENT SYSTEM

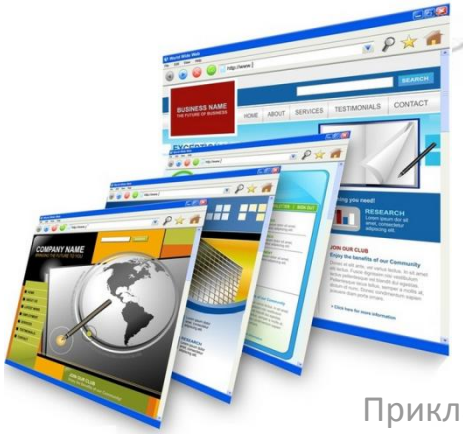
Офисные приложения
(Microsoft Office)



Издательские системы (Quark Publishing System)



СУБД (Oracle Berkeley DB XML)

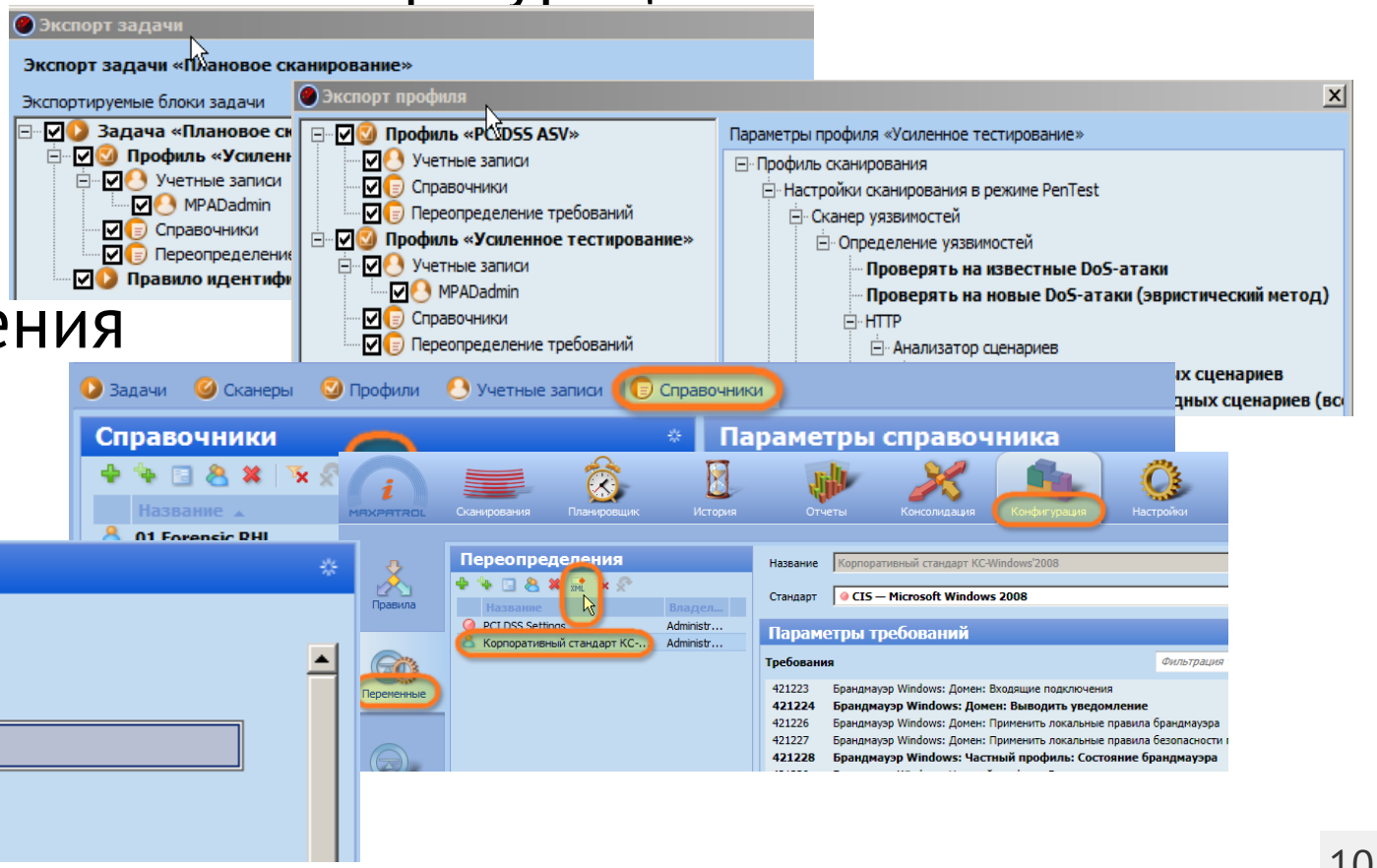


Прикладное ПО (LMS,
сервисные утилиты и пр.)

Сервера управления
контентом (MarkLogic Server)

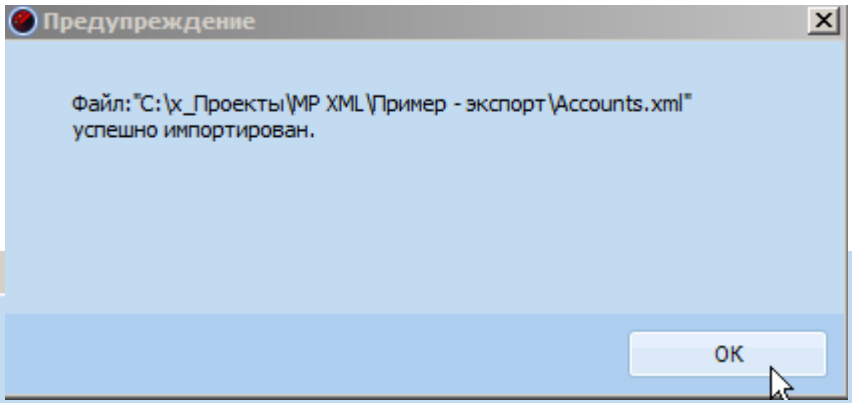
XML в MaxPatrol: управление конфигурацией

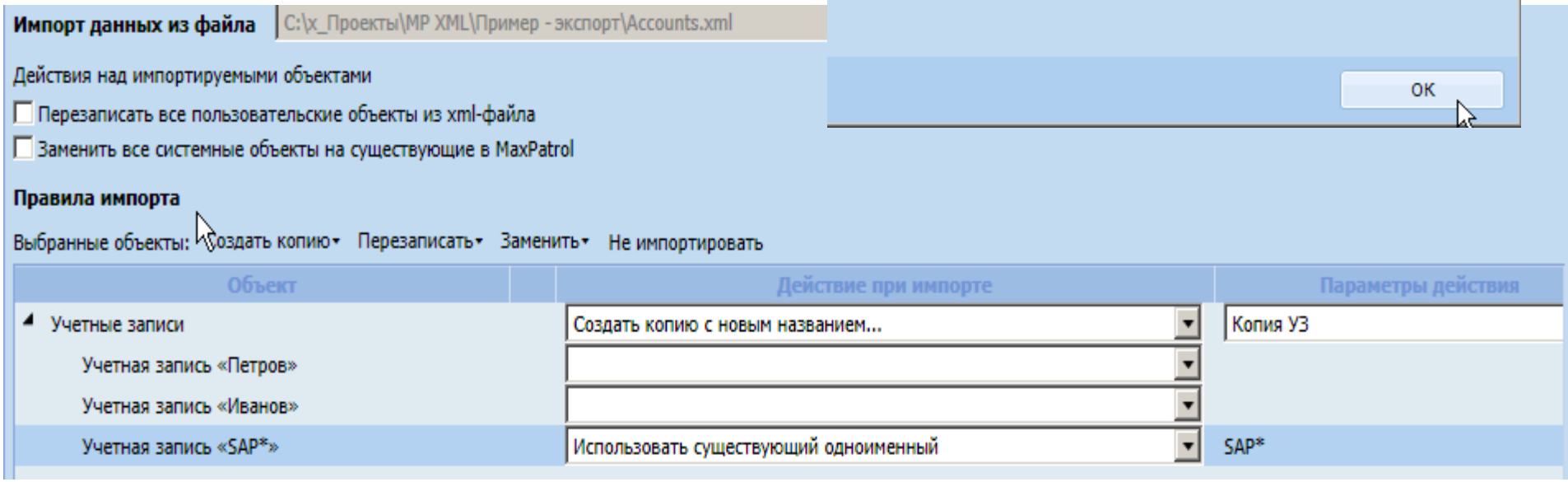
Сохранение эталонной конфигурации:
- справочники
- профили
- задачи
- переопределения
- стандарты



XML в MaxPatrol: управление конфигурацией

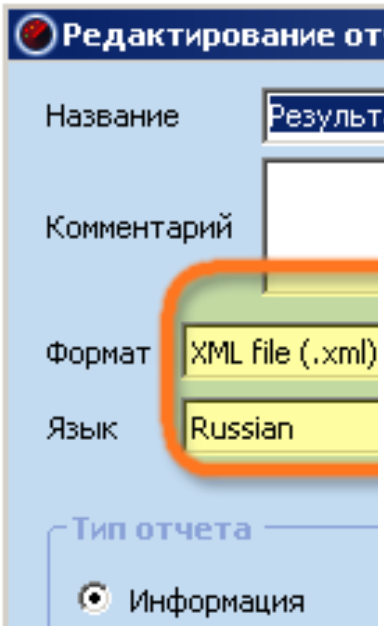
Получение конфигурационных файлов





XML в MaxPatrol: система отчетности

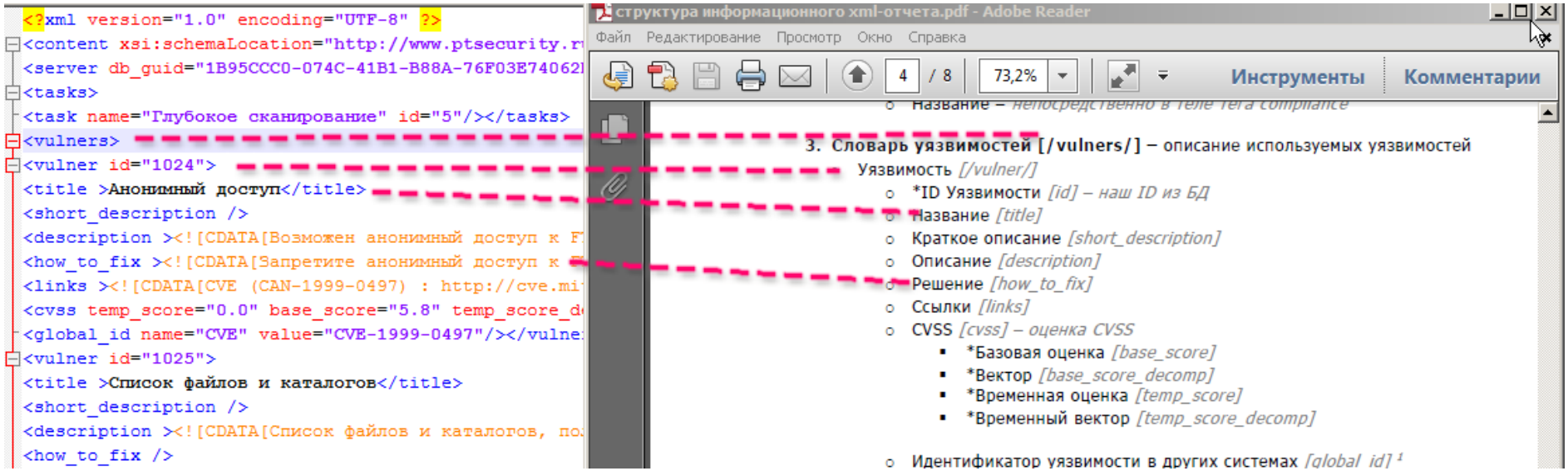
Формирование XML-отчета




```
<?xml version="1.0" encoding="UTF-8" ?>
- <content xsi:schemaLocation="http://www.ptsecurity.ru/reports https://support.ptsecurity.ru/xsd/mp8/23/maxpatrol80-info-report.xsd" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="http://www.ptsecurity.ru/reports" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <server db_guid="1B95CCC0-074C-41B1-B88A-76F03E74062D" license="5640" id="1" version="14975" />
  - <tasks>
    <task name="Глубокое сканирование" id="5" />
  </tasks>
  - <vulners>
    - <vulner id="1024">
      <title>Анонимный доступ</title>
      <short_description />
      - <description>
        <![CDATA[ Возможен анонимный доступ к FTP-серверу. При определенных условиях это может привести к потере данных. ]]>
      </description>
      - <how_to_fix>
        <![CDATA[ Запретите анонимный доступ к FTP-серверу, если в нем нет необходимости. ]]>
      </how_to_fix>
      - <links>
        <![CDATA[ CVE (CAN-1999-0497) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0497 ]]>
      </links>
      <cvss temp_score="0.0" base_score="5.8" temp_score_decomp="" base_score_decomp="(AV:N/AC:M/Au:N/C:P/I:P/A:N)" />
      <global_id name="CVE" value="CVE-1999-0497" />
    </vulner>
```

XML в MaxPatrol: система отчетности

Формирование XML-отчета

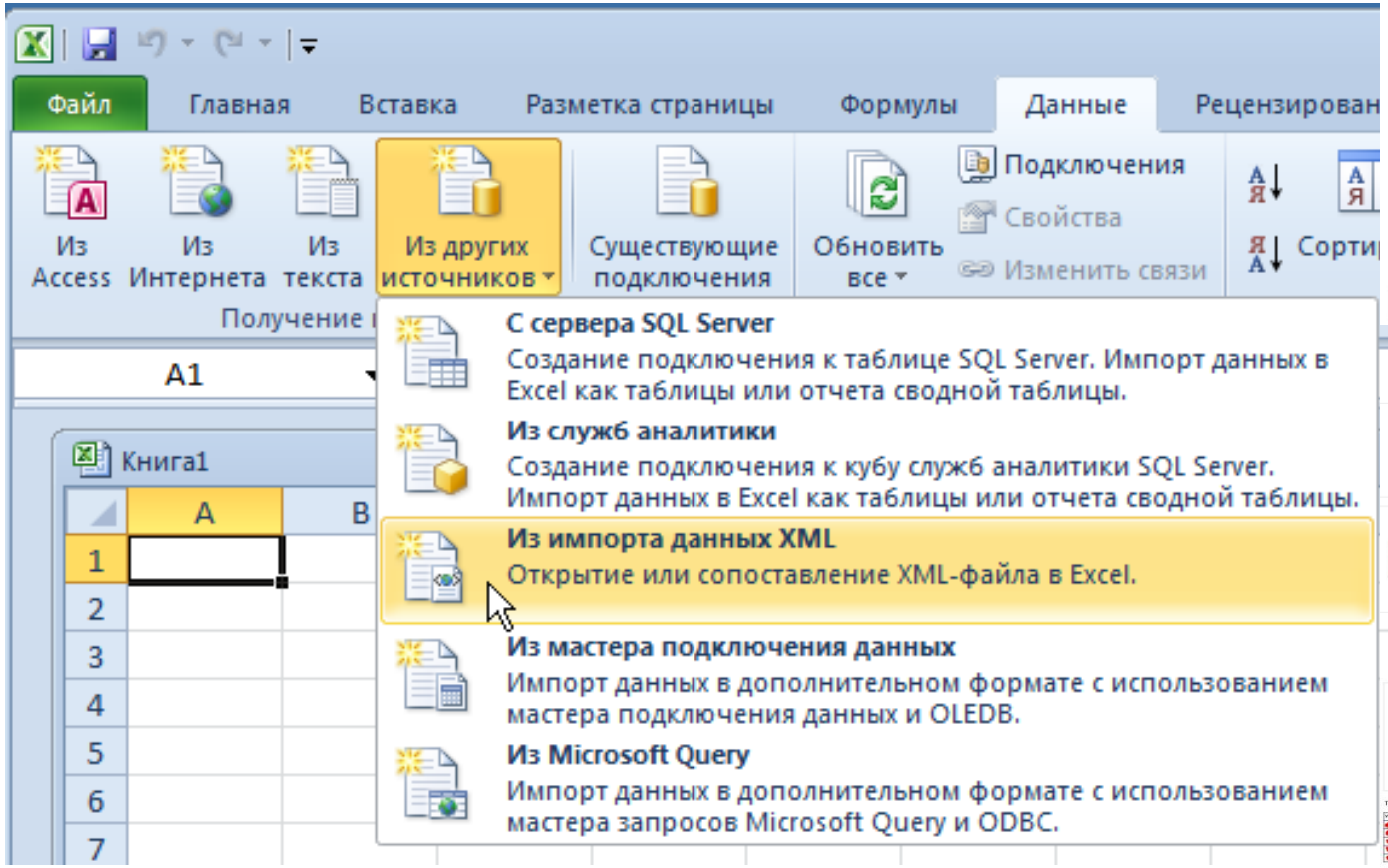


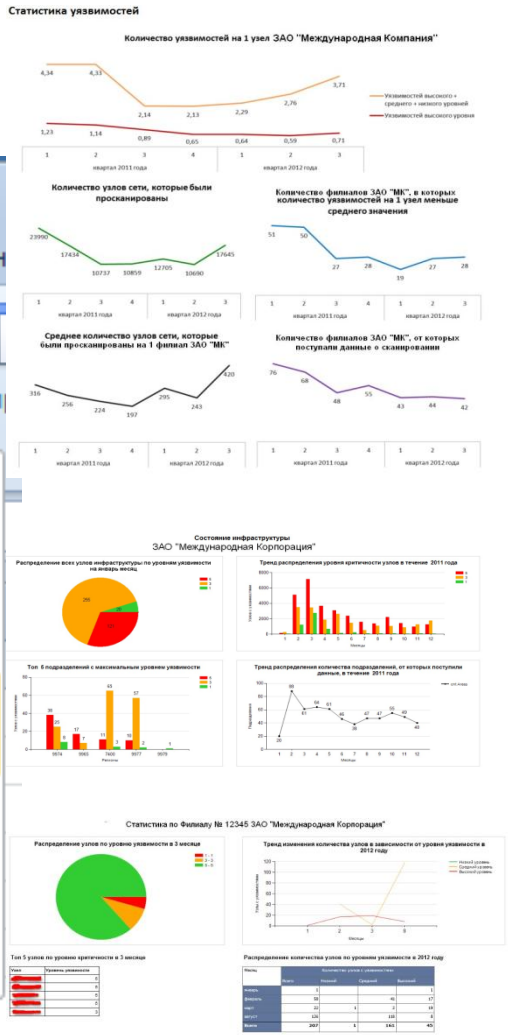
Структура дифференциального XML-отчета
Во вложении.

Структура информационного XML-отчета
Во вложении.

XML в MaxPatrol: система отчетности

Обработка XML-отчета в Excel

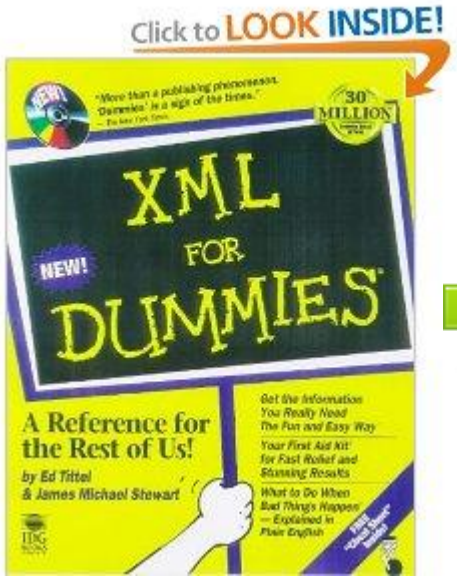


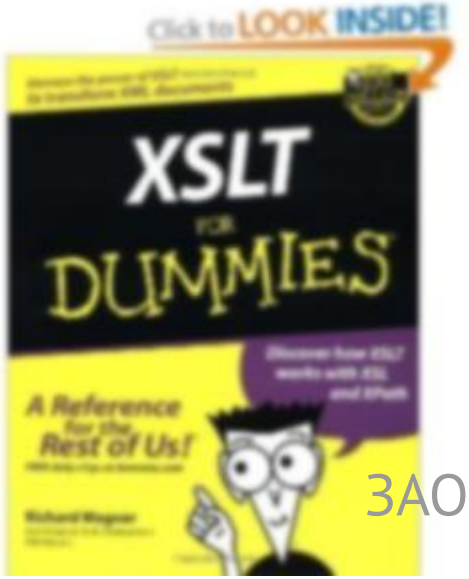


POSITIVE TECHNOLOGIES

Часть 2.
XML для «чайников»

Гроссмейстер пошел e2-e4





Павел Лысов

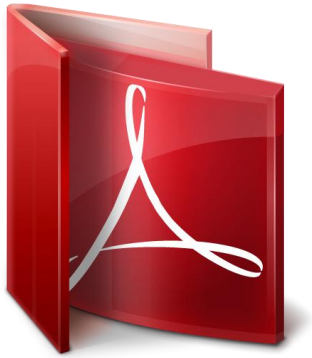
старший программист

ЗАО «Positive Technologies»

MHT/PDF кому мало?

MHT
веб-архив

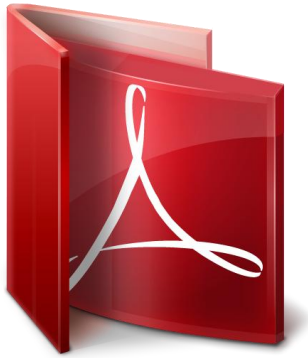
PDF

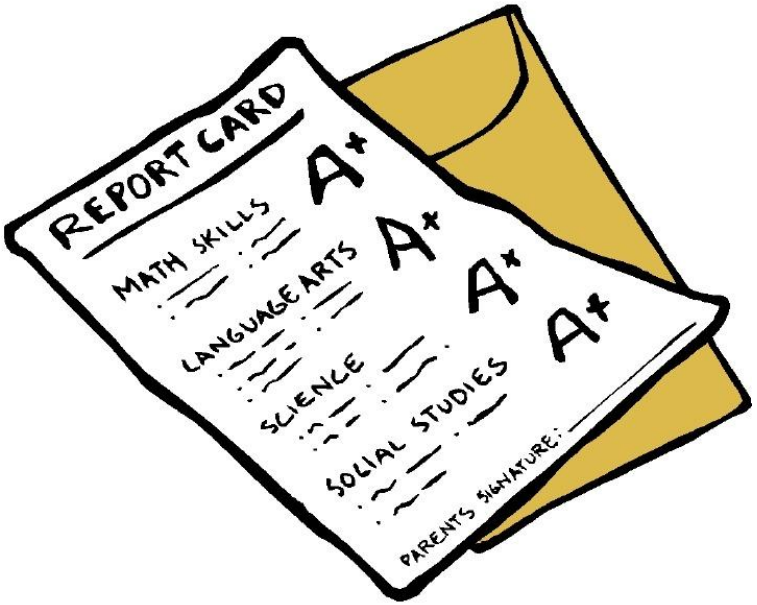


MHT/PDF кому мало?

MHT
веб-архив

PDF



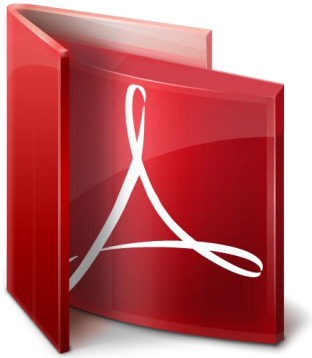


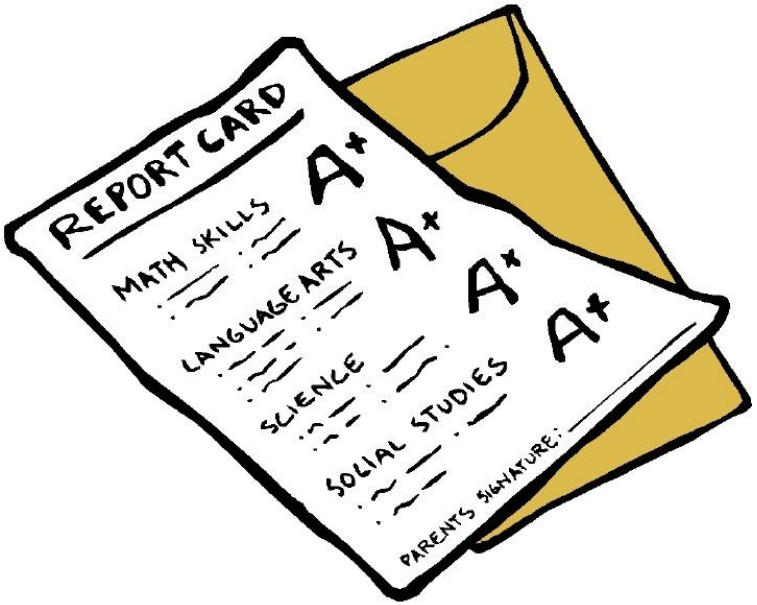
Плюсы и минусы, а есть ли они?

MHT/PDF кому мало?

MHT
веб-архив

PDF





Плюсы и минусы, а есть ли они?

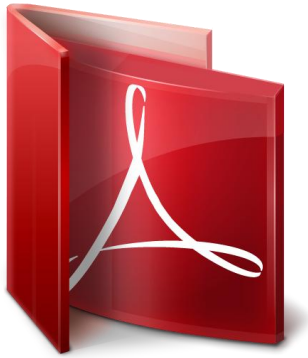
“плюсы”:

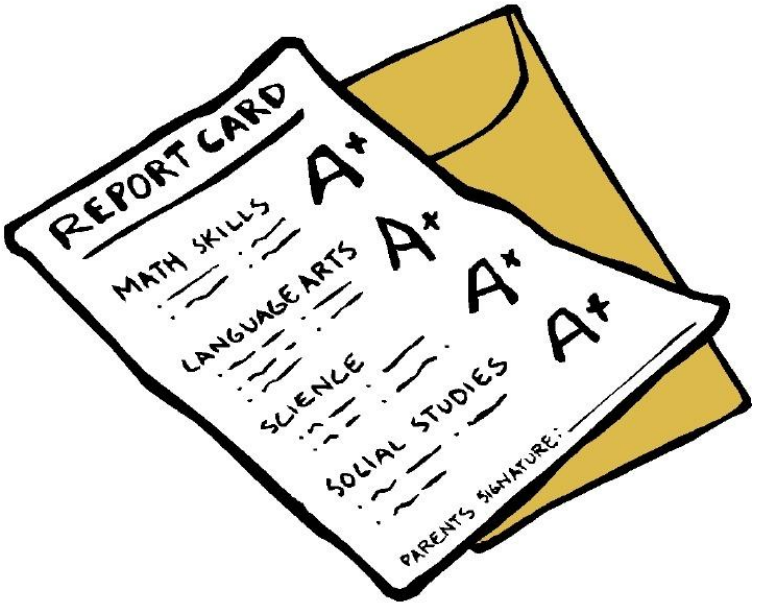
- это красиво =)

MHT/PDF кому мало?

MHT
веб-архив

PDF





Плюсы и минусы, а есть ли они?

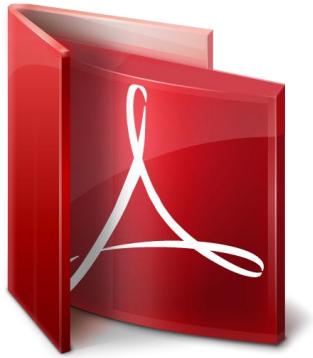
“плюсы”:

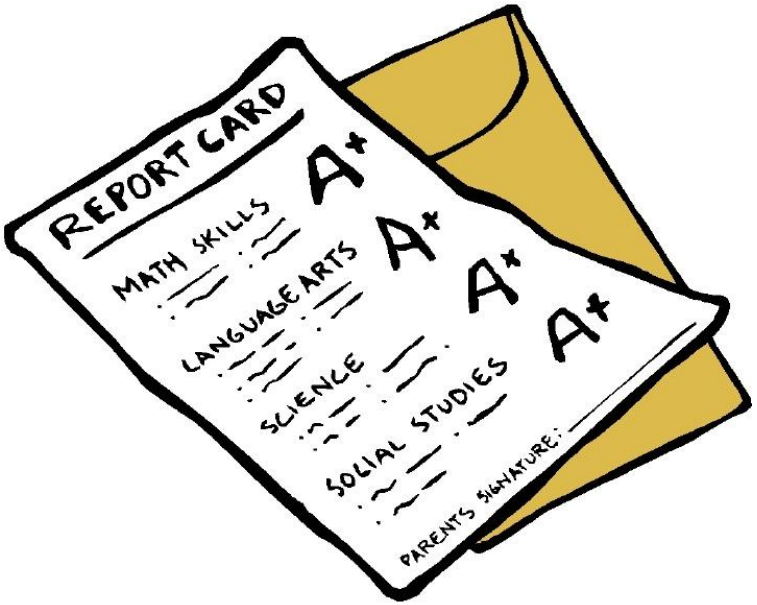
- это красиво =)
- вариант из коробки

MHT/PDF кому мало?

MHT
веб-архив

PDF





Плюсы и минусы, а есть ли они?

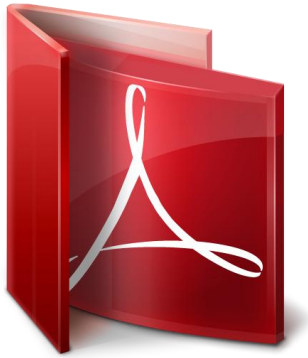
“плюсы”:

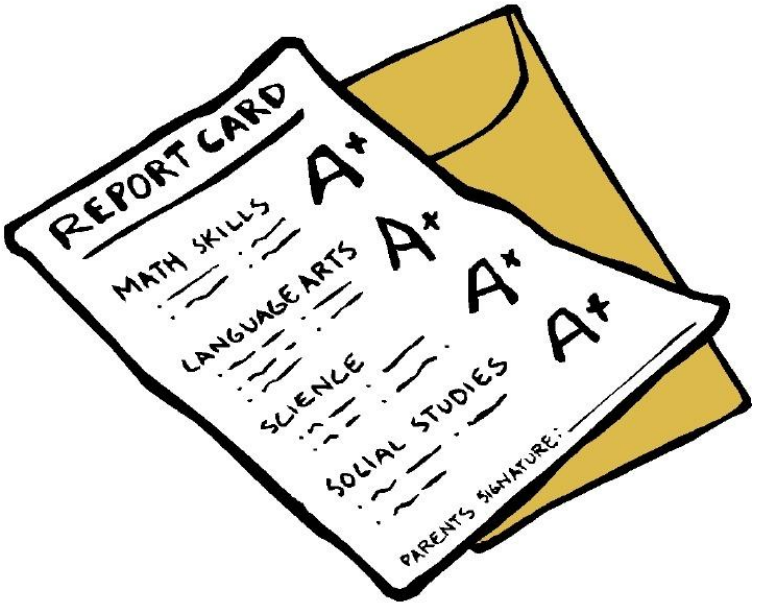
- это красиво =)
- вариант из коробки
- можно отправить на принтер

MHT/PDF кому мало?

MHT
веб-архив

PDF





Плюсы и минусы, а есть ли они?

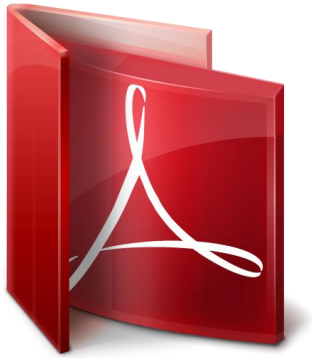
“плюсы”:

- это красиво =)
- вариант из коробки
- можно отправить на принтер
- элементы управления и навигации

MHT/PDF кому мало?

MHT
веб-архив

PDF

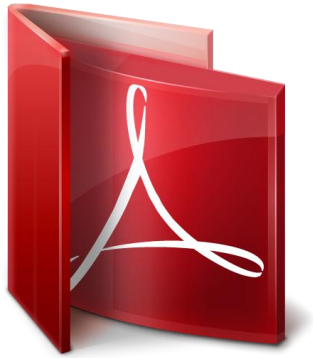


А что по поводу минусов?

MHT/PDF кому мало?

MHT
веб-архив

PDF



А что по поводу минусов?

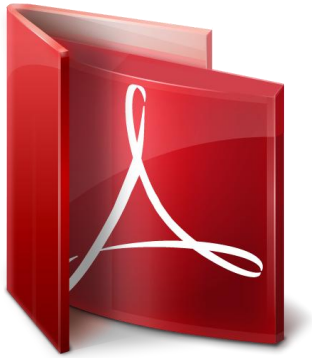
“минусы”:

- только для чтения

MHT/PDF кому мало?

MHT
веб-архив

PDF



А что по поводу минусов?

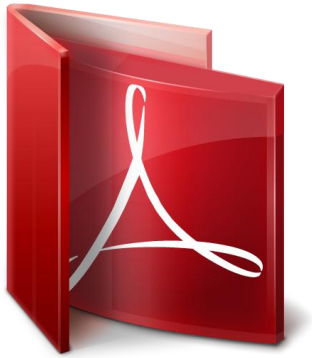
“минусы”:

- только для чтения
- большой размер отчета

MHT/PDF кому мало?

MHT
веб-архив

PDF



А что по поводу минусов?

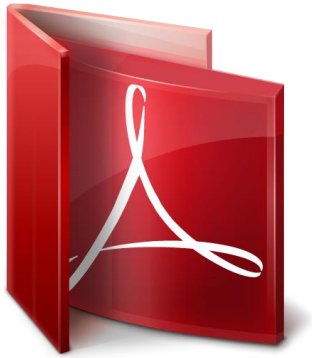
“минусы”:

- только для чтения
- большой размер отчета
- отсутствие гибкости

MHT/PDF кому мало?

MHT
веб-архив

PDF



А что по поводу минусов?

“минусы”:

- только для чтения
- большой размер отчета
- отсутствие гибкости
- не для интеграции

POSITIVE TECHNOLOGIES

XML, альтернатива ли?

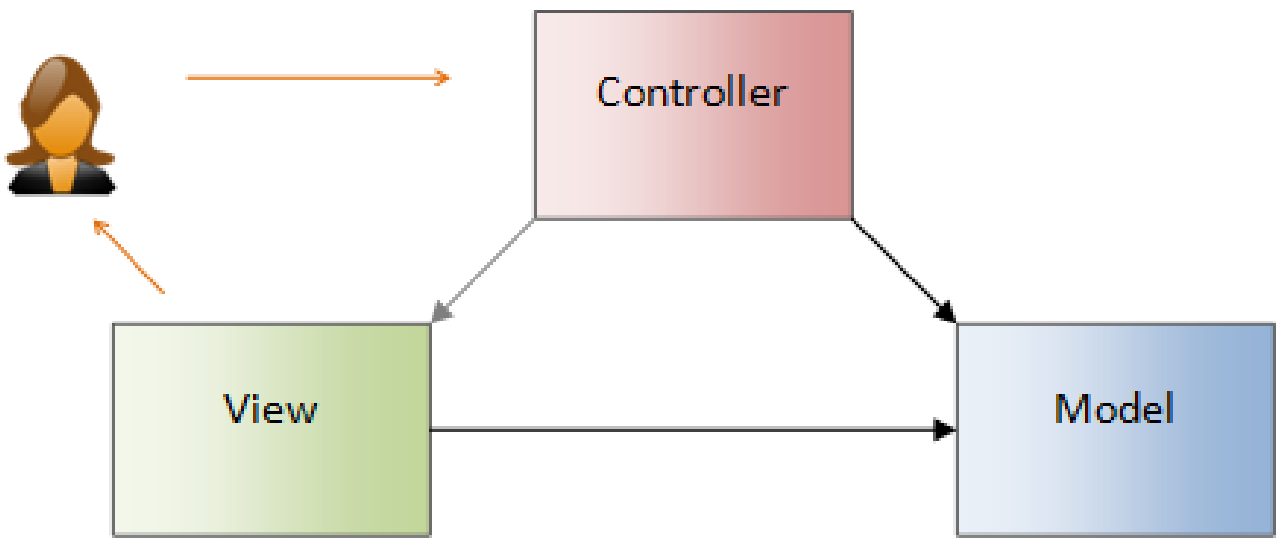
XML-отчет противоположность MHT/PDF:

```
<?xml version="1.0" encoding="UTF-8" ?>
- <content xsi:schemaLocation="http://www.ptsecurity.ru/reports
    https://support.ptsecurity.ru/xsd/mp8/24/maxpatrol80-info-report.xsd"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns="http://www.ptsecurity.ru/reports"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <server db_guid="E85A650A-4E81-42AC-8D06-FD08EE1BDEB3" license="1588" id="1"
      version="13884" />
  - <tasks>
      <task name="+10.111.113.67" id="18" />
    </tasks>
  + <vulners>
  - <data>
    - <host ip="10.111.113.67" start_time="2011-09-19T20:31:25Z" task="18"
        host_uid="1" scan="48" fqdn="" stop_time="2011-09-19T20:51:54Z"
        primary="10.111.113.67" exitcode="0" scan_status="0" netbios="">
        <qualifier_rule>As specified</qualifier_rule>
        <scanner version="10050">Default Scanner on IMAKSIMO-G8QPNI</scanner>

          <transport_info>WMI:4/FILESYSTEM:4/RPC:4/LDAP:1/SSH:2/TELNET:4/SQL:4/O
          REGISTRY:4/WMI REGISTRY:4/NOTES RPC:4/WMI FILESYSTEM:0/REMOTE
          ENGINE:0</transport_info>
      + <hardware name="Hardware Information" security_object="6075071">
      + <scan_objects>
      </host>
    </data>
  </content>
```

MVC – это просто!

Model-view-controller (**MVC**, «Модель-представление-контроллер»)



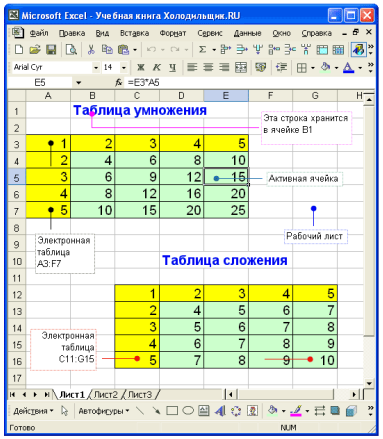
- **Контроллер** – конструктор отчетов MaxPatrol
- **Модель** – XML-отчет
- **Представление** - ?

Представление XML, как использовать?

Киса, разрешите спросить вас как художник художника… Вы рисовать умеете?

— CSS - *Cascading Style Sheets* — каскадные таблицы стилей

— Excel – как инструмент работы с таблицами



POSITIVE TECHNOLOGIES

Представление XML, как использовать?

А может тебе дать еще ключ от квартиры, где деньги лежат?!!!

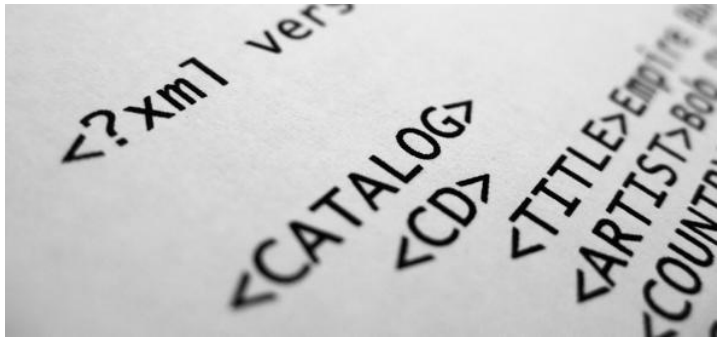
— Интеграция с внешними системами (ArcSight, SkyBOX Security Risk Control и т.д.)

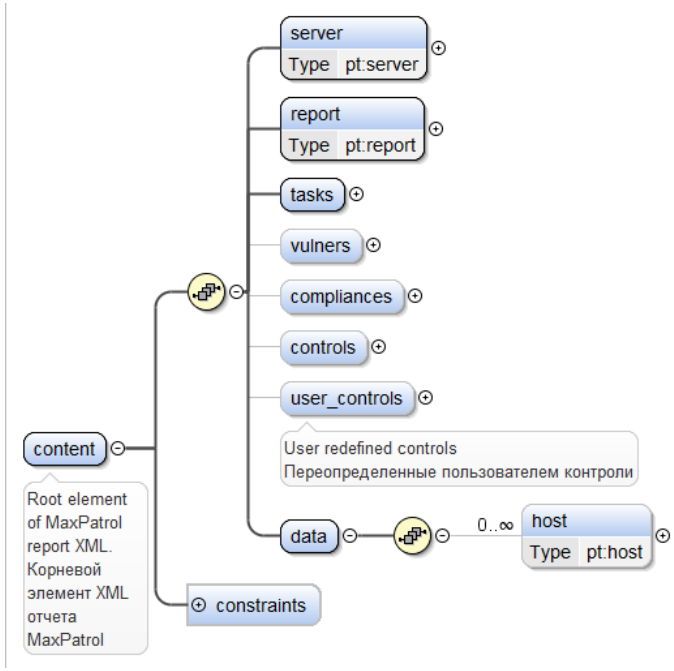
— Интеграция с внешними системами отчетности (MS Reporting Services, Crystal Reports, Fast Reports и т.д.)

Excel для представления XML отчетов?

— Импорт RAW данных из XML

— Карта XML, она же схема XSD





POSITIVE TECHNOLOGIES

Импорт сырых данных из XML.

Да, это вам не Рио-де-Жанейро!

	A	B	C	D	E	F	G	H
1	db_guid	license	id	version	name	id2	id3	ns1:title
2	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.113.67	18	7003	Stack-Based Buffer Overflow
3	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.113.67	18	100620	Multiple Vulnerabilities
4	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.113.67	18	100620	Multiple Vulnerabilities
5	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.113.67	18	100620	Multiple Vulnerabilities
6	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.113.67	18	100620	Multiple Vulnerabilities
7	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.113.67	18	100621	Multiple Vulnerabilities (Samba)
8	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.113.67	18	100621	Multiple Vulnerabilities (Samba)
9	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.113.67	18	100621	Multiple Vulnerabilities (Samba)
10	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.113.67	18	100627	Cache Poisoning Vulnerability
11	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.113.67	18	100627	Cache Poisoning Vulnerability
12	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.113.67	18	100627	Cache Poisoning Vulnerability
13	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.113.67	18	100627	Cache Poisoning Vulnerability
14	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.113.67	18	100627	Cache Poisoning Vulnerability
15	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.113.67	18	100627	Cache Poisoning Vulnerability
16	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.113.67	18	100627	Cache Poisoning Vulnerability
17	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.113.67	18	100627	Cache Poisoning Vulnerability
18	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.113.67	18	100627	Cache Poisoning Vulnerability
19	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.113.67	18	100627	Cache Poisoning Vulnerability
20	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.113.67	18	100627	Cache Poisoning Vulnerability

Импорт XML с картой

Берегите пенсне, Киса! Сейчас начнется!

Где взять карту XML?

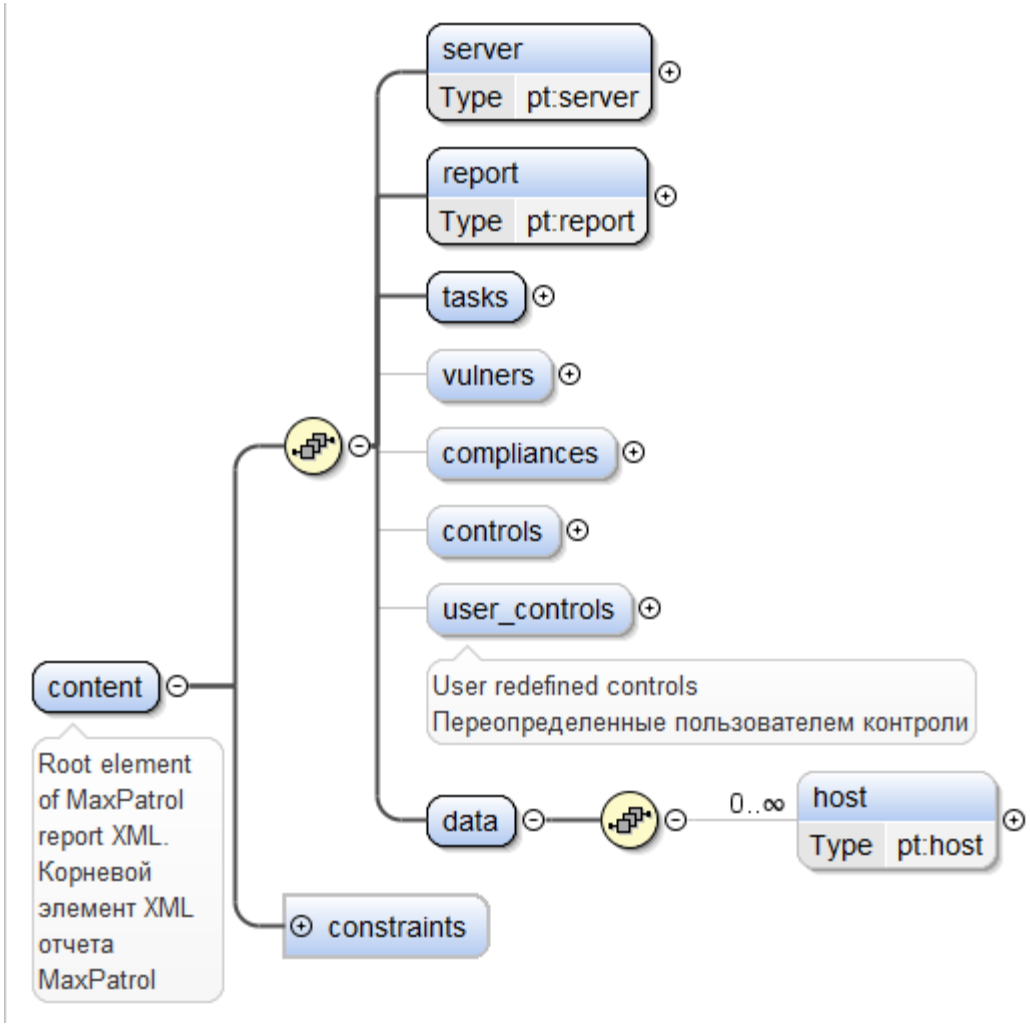
— Удаленно с сайта:

```
<?xml version="1.0" encoding="UTF-8" ?>
- <content xsi:schemaLocation="http://www.ptsecurity.ru/reports
    https://support.ptsecurity.ru/xsd/mp8/24/maxpatrol80-info-report.xsd"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns="http://www.ptsecurity.ru/reports"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

— Локально из консоли MaxPatrol

Импорт XML с картой

Берегите пенсне, Киса! Сейчас начнется!

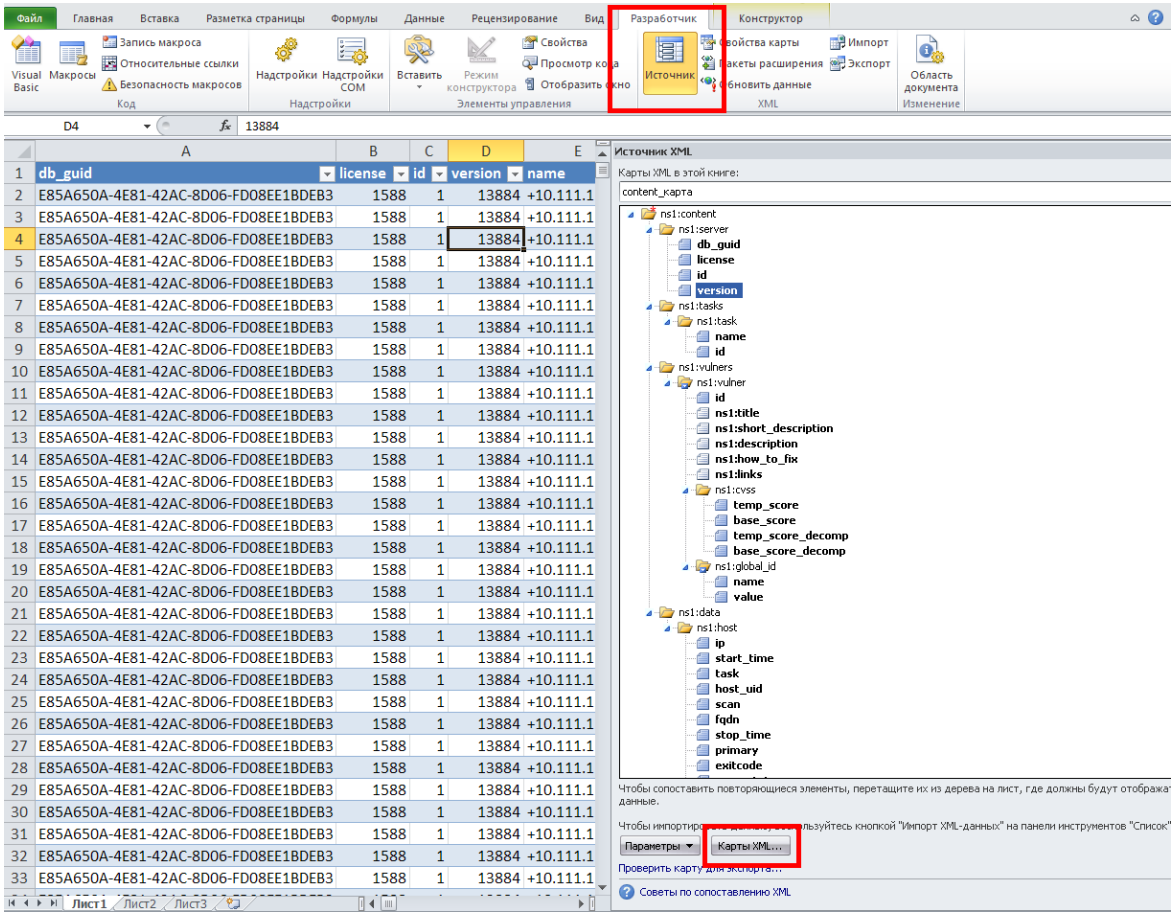


POSITIVE TECHNOLOGIES

Импорт XML с картой

Берегите пенсне, Киса! Сейчас начнется!

— Как воспользоваться картой XML в Excel?



Примеры Excel отчетов

— Отчет по Active Directory

— Дифференциальный отчет

— Сводный отчет по Compliance

	A	B
1	Имя домена	[illegible]
2	Имя группы	Develo
3	Название организационной единицы	[illegible]
4		Имя доменного [illegible]
5		Maxim S[illegible]ky
6		Victor S[illegible]
7		Konstantin K[illegible]ich
8		Vladimir S[illegible]ov
9		Anton S[illegible]r
10		Yury K[illegible]
11		Pavel V[illegible]

A	B	C	D	E	F	G
узел	**задача**	**по уровням уязвимостей**	**добавилось**	**изменилось**	**исчезло**	**не изменилось**
10.111.115.17	PAC_115_17/18	**всего**	2	3	7	14
		всего без подозрений	2	3	7	14
		доступна информация	2	3	7	14
		низкий уровень	0	0	0	0
		средний уровень (подозрение)	0	0	0	0
		средний уровень	0	0	0	0
		высокий уровень (подозрение)	0	0	0	0
		высокий уровень	0	0	0	0
10.111.115.18	PAC_115_17/18	**всего**	2	3	3	18
		всего без подозрений	2	3	3	18
		доступна информация	2	3	3	18
		низкий уровень	0	0	0	0
		средний уровень (подозрение)	0	0	0	0
		средний уровень	0	0	0	0
		высокий уровень (подозрение)	0	0	0	0
		высокий уровень	0	0	0	0
По всем узлам	Узлов: 2	**всего**	4	6	10	32
		всего без подозрений	4	6	10	32

POSITIVE TECHNOLOGIES

Итоги. Части 2.

Использование формата XML позволило решить проблемы:

- Интеграции
- Редактируемого формата

Остались проблемы:

- Отсутствие гибкости
- Большой размер отчета

POSITIVE TECHNOLOGIES

Часть 3.
X-MAN

Командовать парадом буду я!

Павел Лысов

старший программист

ЗАО «Positive Technologies»

POSITIVE TECHNOLOGIES

Использование XSLT и XPath.

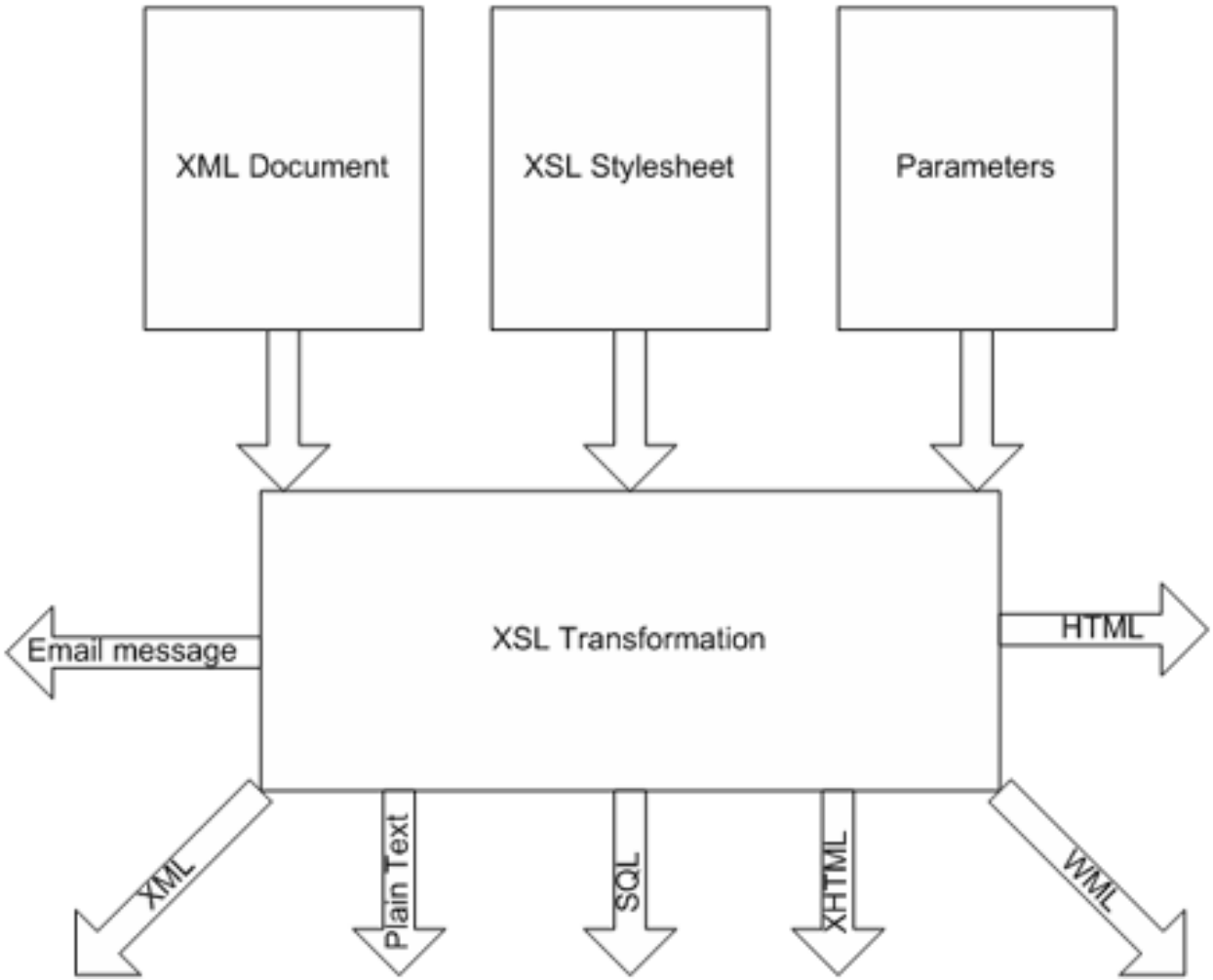
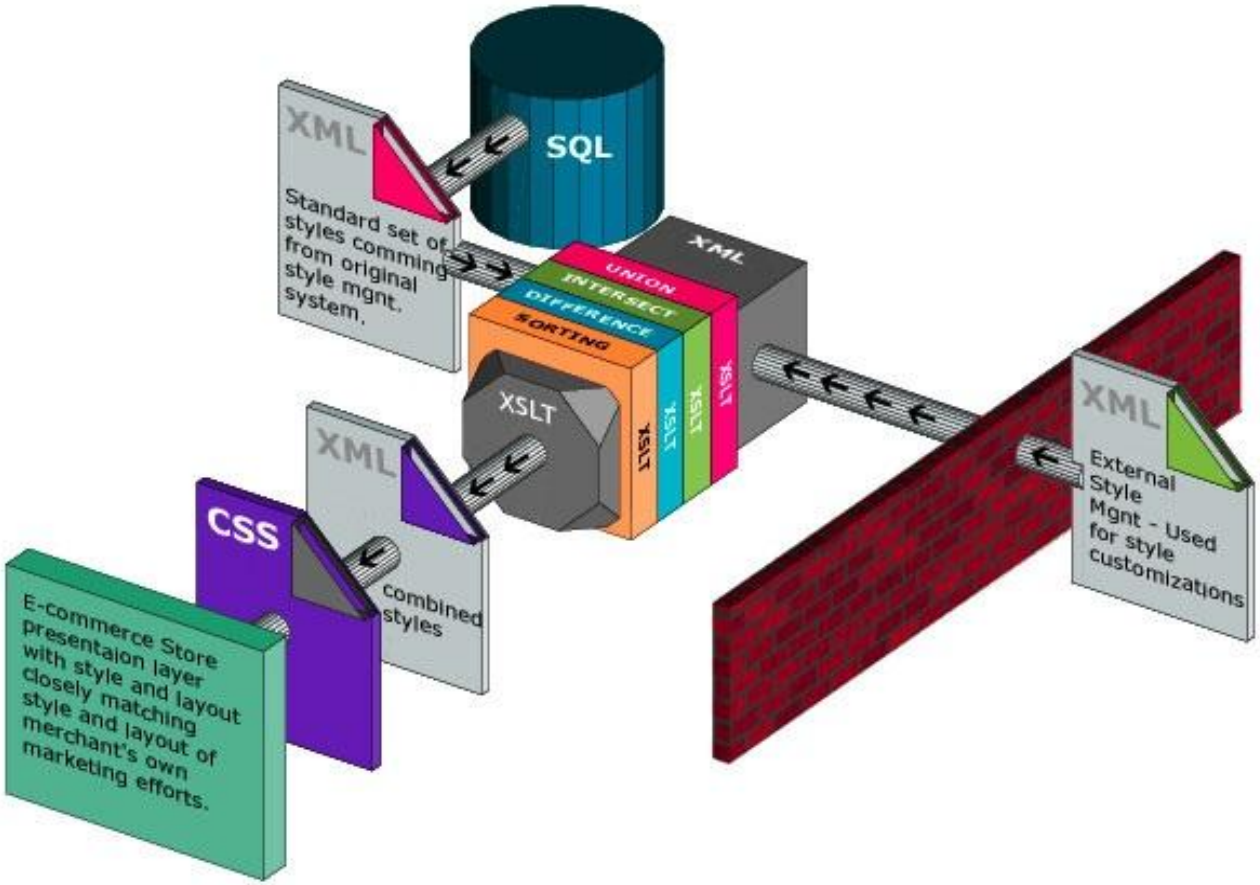
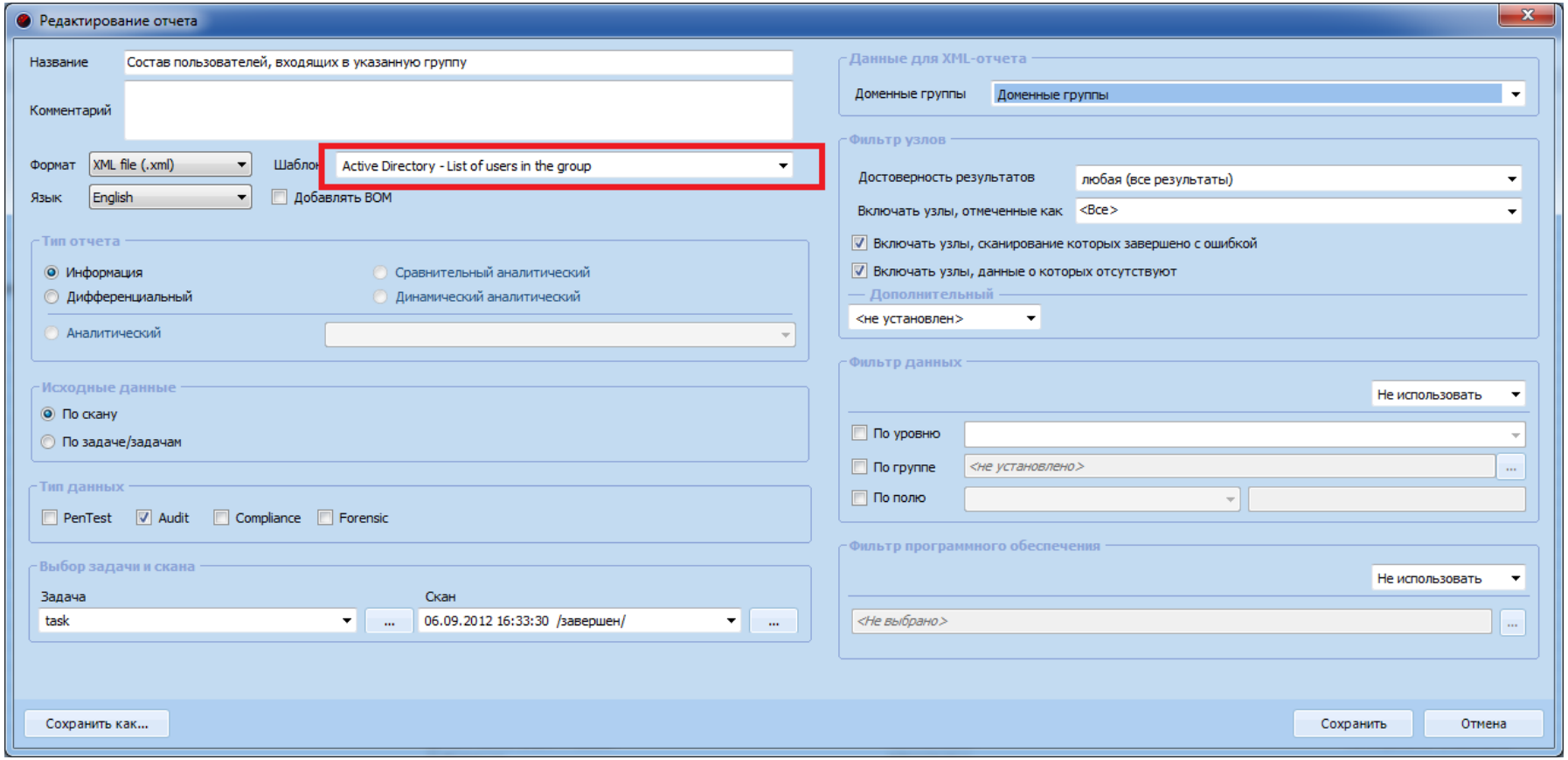


Схема работы генератора отчета в формате XML MaxPatrol 8.0 с использованием XSLT шаблона



Как применить XSLT в MaxPatrol?



POSITIVE TECHNOLOGIES

Пример отчета PCI DSS ASV. Видео.

	A	B	C	D
1	**Scan Customer Information**		**Approved Scanning Vendor Information**	
2	Company:	_Positive Technologies	Company:	Positive Technologies
3	Contact:	_Yury Maksimov	Contact:	Yury Maksimov
4	Title:	_PT	Title:	PT
5	Telephone:	_+7 (495) 744-0144	Telephone:	+7 (495) 744-0144
6	E-mail:	_ym@ptsecurity.ru	E-mail:	ym@ptsecurity.ru
7	Business Address:	_Shchelkovskoe shosse, 23A	Business Address:	Shchelkovskoe shosse, 23A
8	City:	_Moscow	City:	Moscow
9	State/Province:	_	State/Province:	
10	ZIP:	_107241	ZIP:	107241
11	URL:	_ptsecurity.ru	URL:	ptsecurity.ru
12				
13	**Scan Status**			
14	Compliance Status			Fail
15	Number of unique components scanned:			1
16	Number of identified failing vulnerabilities:			1
17	Number of components found by ASV but not scanned because scan customer confirmed components were out of scope:			0
18	Date scan completed:			27.11.2012
19	Scan expiration date (90 days from date scan completed):			25.02.2013
20				
21	**Scan Customer Attestation**			
	_*Positive Technologies* attests on *2012-11-27* that this scan includes all components which should be in scope for PCI DSS, any component considered out-of-scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions is accurate and complete. _*Positive Technologies* also acknowledges the following: 1) proper scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.			
22				
23				
24	**ASV Attestation**			
	This scan and report was prepared and conducted by *Positive Technologies* under certificate number *1*, according to internal processes that meet PCI DSS requirement 11.2 and the PCI DSS ASV Program Guide. *Positive Technologies* attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, and 3) active scan interference. This report and any exceptions were reviewed by *Dmitry Evteev*.			

POSITIVE TECHNOLOGIES

Итоги. Части 3.

Использование формата XML + XSLT позволило решить проблемы:

- Интеграции
- Редактируемого формата
- Гибкость
- Большой размер отчета

POSITIVE TECHNOLOGIES

Часть 4.
Reporting Services

Заседание продолжается!

Павел Лысов

старший программист

ЗАО «Positive Technologies»

POSITIVE TECHNOLOGIES

В чем соль?

POSITIVE TECHNOLOGIES

В чем соль?

- Работа с большими объемами данных

POSITIVE TECHNOLOGIES

В чем соль?

- Работа с большими объемами данных
- Дополнительные расчеты (пользовательские метрики, KPI)

POSITIVE TECHNOLOGIES

В чем соль?

- Работа с большими объемами данных
- Дополнительные расчеты (пользовательские метрики, KPI)
- Специальные отчеты (с учетом иерархии инфраструктуры)

В чем соль?

- Работа с большими объемами данных
- Дополнительные расчеты (пользовательские метрики, KPI)
- Специальные отчеты (с учетом иерархии инфраструктуры)
- Доступ по WEB

POSITIVE TECHNOLOGIES

В чем соль?

- Работа с большими объемами данных
- Дополнительные расчеты (пользовательские метрики, KPI)
- Специальные отчеты (с учетом иерархии инфраструктуры)
- Доступ по WEB
- Интерактивность

POSITIVE TECHNOLOGIES

Как это работает?

POSITIVE TECHNOLOGIES

Как это работает?

- Производится сканирование MaxPatrol

POSITIVE TECHNOLOGIES

Как это работает?

- Производится сканирование MaxPatrol
- Выпускается отчетность в формате XML

POSITIVE TECHNOLOGIES

Как это работает?

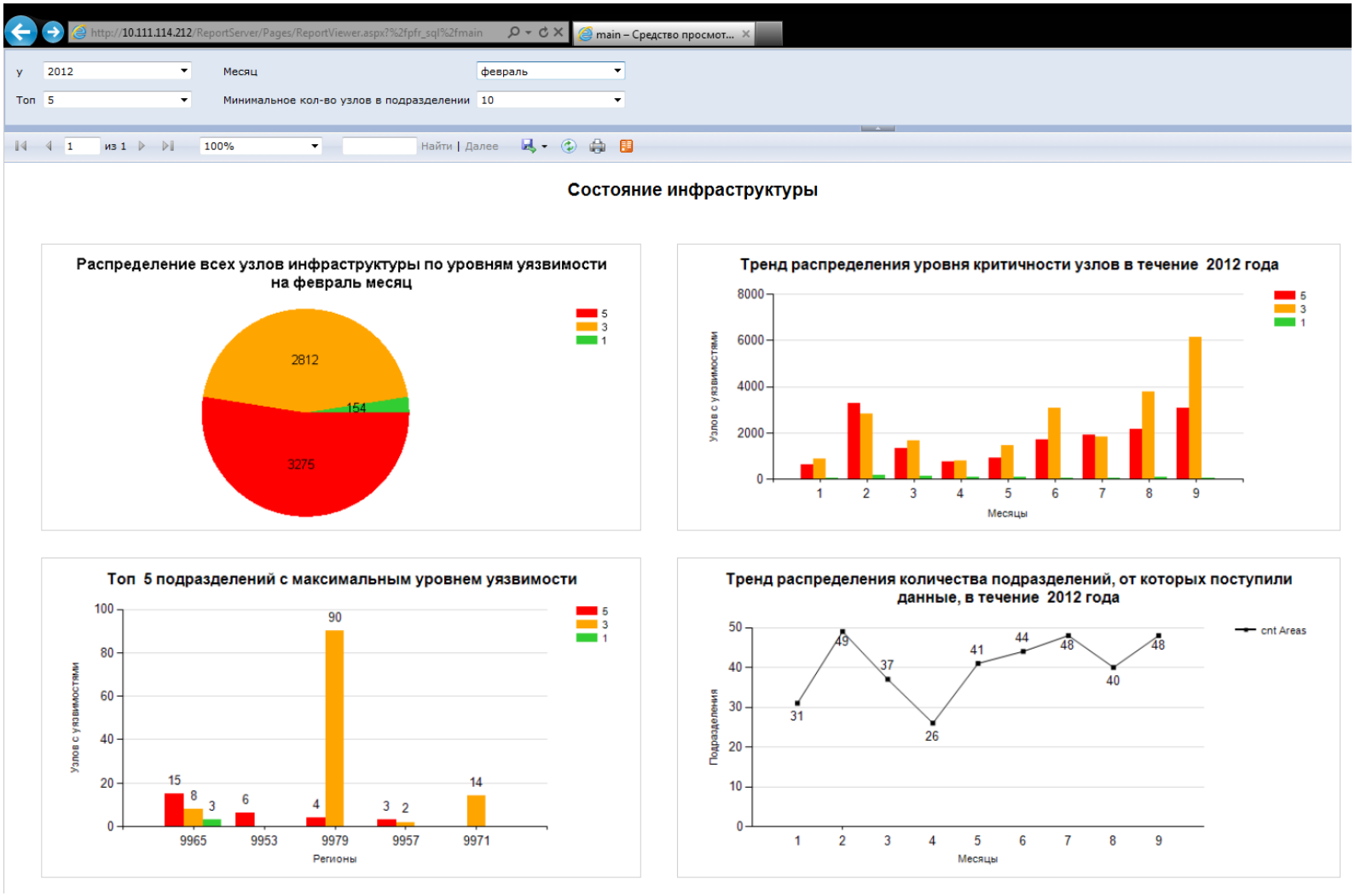
- Производится сканирование MaxPatrol
- Выпускается отчетность в формате XML
- Производится импорт данных во внешнюю БД

POSITIVE TECHNOLOGIES

Как это работает?

- Производится сканирование MaxPatrol
- Выпускается отчетность в формате XML
- Производится импорт данных во внешнюю БД
- Данные отображаются на Web-странице отчета

Пример. Видео.



POSITIVE TECHNOLOGIES

Конец рассказа
Спасибо за внимание

Александр Веретенников
averetennikov@ptsecurity.ru

Павел Лысов
plysov@ptsecurity.ru