

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»

Часть 1.

Введение

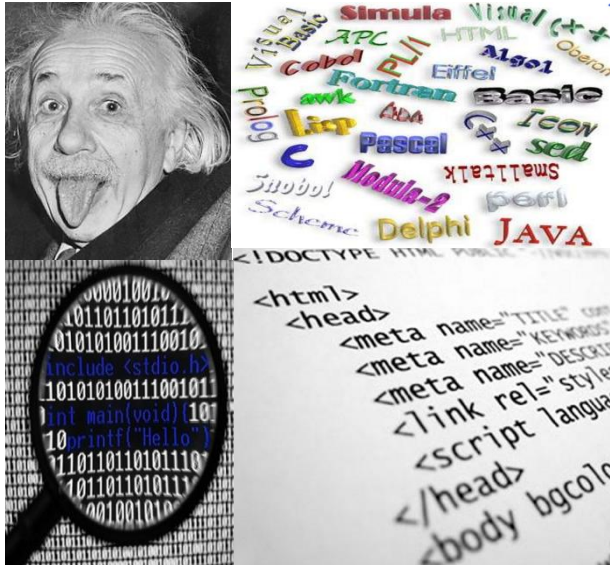
Александр Веретенников

консультант

ЗАО «Positive Technologies»

Такие разные ... «ЯЗЫКИ»

Albert Einstein versus ГОСТ Р 52292-2004



Язык разметки XML: общая информация

У работе
КОМСОМОЛА
на селе

Текст (для
собственных нужд)

Пишу КАК
считаю
НЕЖНЫМ
!

Текст (для
публикации)

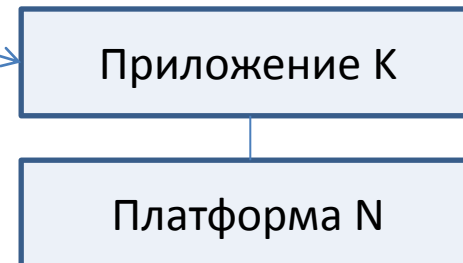
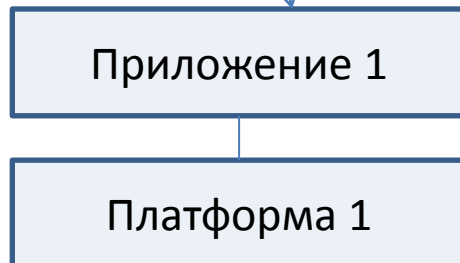
Записывать текст по
установленным правилам, с
заданным оформлением!



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.



Mr.XML, who are you?

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)

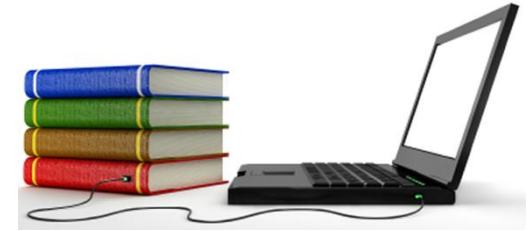
```
<?xml version="1.0" encoding="UTF-8"
- <Contato>
  <id>100</id>
  <nome>Fulano da Silva</nome>
  <email>fulano@email.com</email>
- <Telefones>
  - <Telefone>
    <id>1</id>
    <ddd>55</ddd>
    <numero>32214512</numero>
  </Telefone>
  - <Telefone>
    <id>2</id>
    <ddd>55</ddd>
    <numero>99879885</numero>
  </Telefone>
</Telefones>
- <Endereco>
  <id>11</id>
  <logradouro>Rua dos Javanezes<
  <bairro>Largo Zero</bairro>
  <cep>97010600</cep>
  <cidade>Java City</cidade>
  <complemento>Ap.103A</complem
  <numero>65</numero>
  </Endereco>
</Contato>
```

XML : ДОБРО ПОЖАЛОВАТЬ!

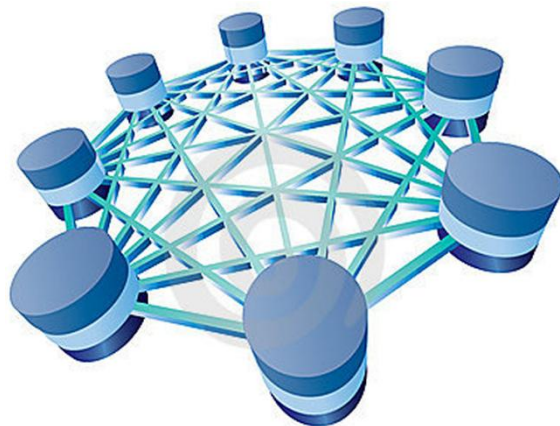


Офисные приложения
(Microsoft Office)

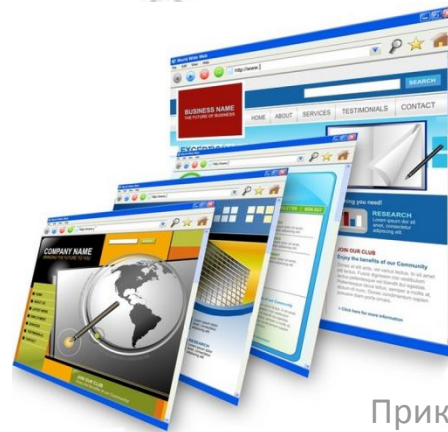
XML



Издательские системы (Quark
Publishing System)



СУБД (Oracle Berkeley DB XML)



Прикладное ПО (LMS,
сервисные утилиты и пр.)



Сервера управления
контентом (MarkLogic Server)

MAXPATROL

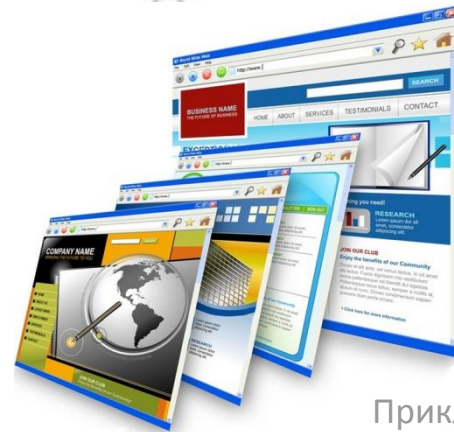
VULNERABILITY AND COMPLIANCE MANAGEMENT SYSTEM



Издательские системы (Quark Publishing System)



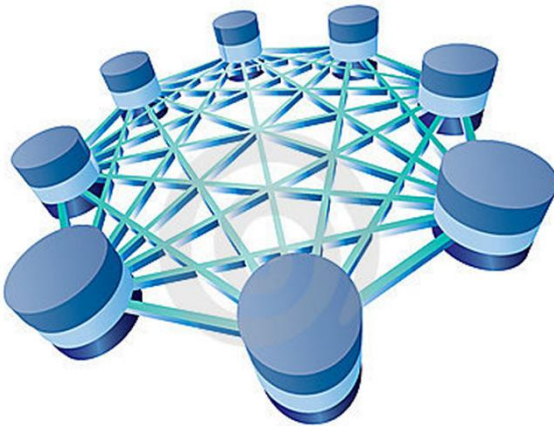
Сервера управления контентом (MarkLogic Server)



Прикладное ПО (LMS, сервисные утилиты и пр.)



Офисные приложения (Microsoft Office)

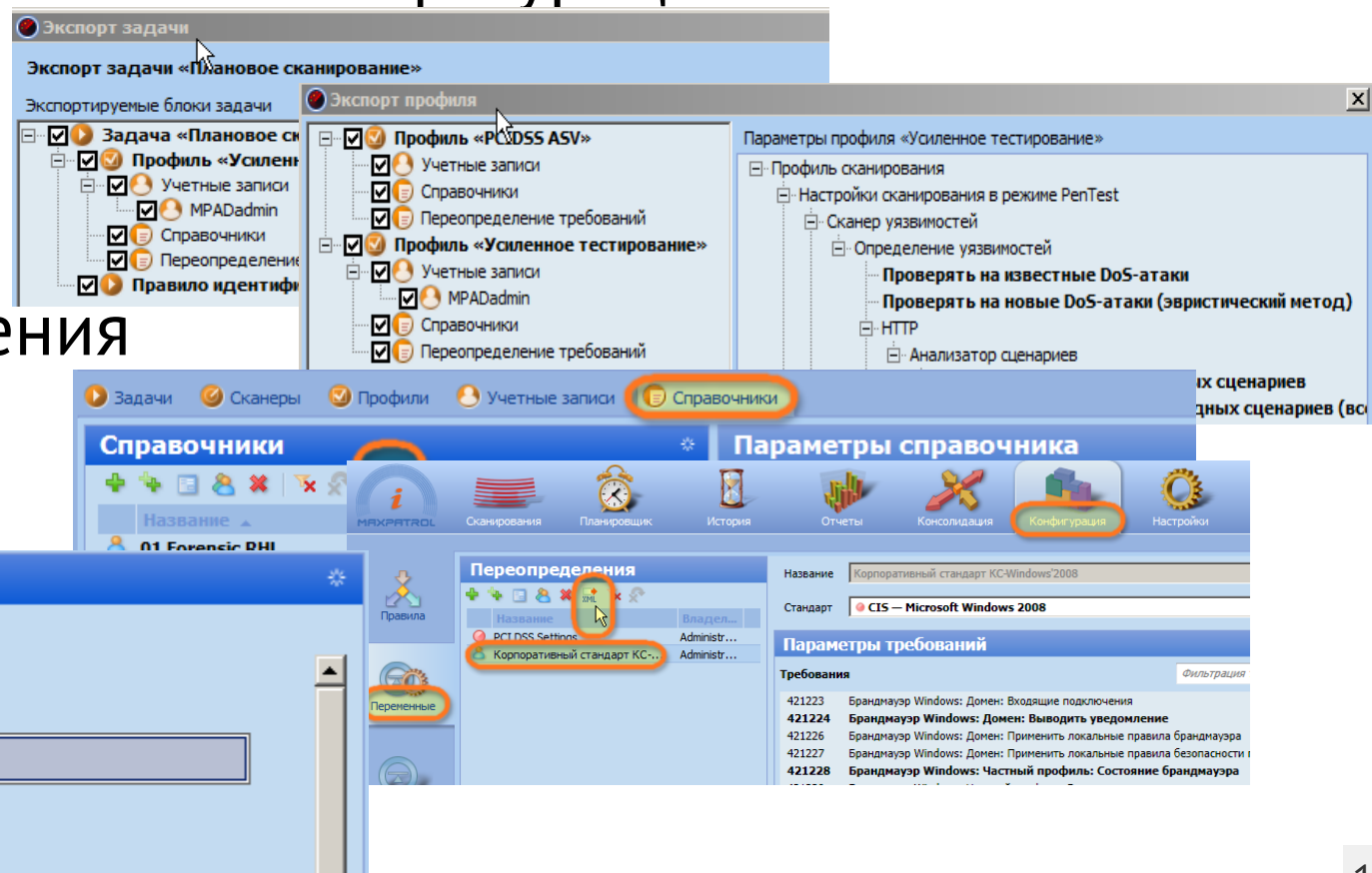


СУБД (Oracle Berkeley DB XML)

XML в MaxPatrol: управление конфигурацией

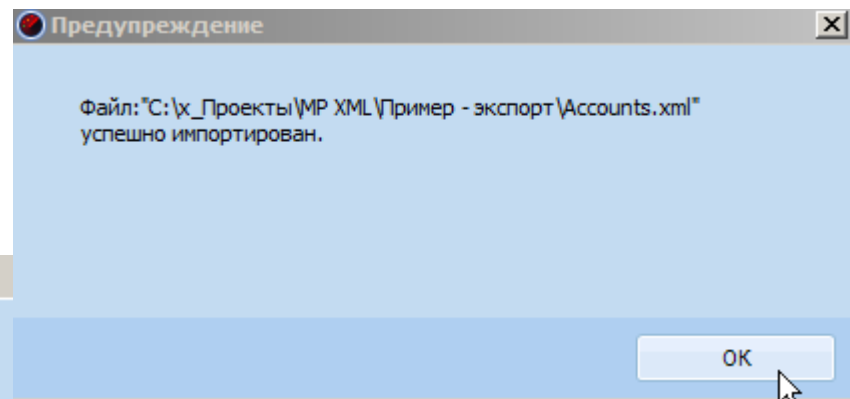
Сохранение эталонной конфигурации:

- справочники
- профили
- задачи
- переопределения
- стандарты



XML в MaxPatrol: управление конфигурацией

Получение конфигурационных файлов



Импорт данных из файла | C:\x_Проекты\MP XML\Пример - экспорт\Accounts.xml

Действия над импортируемыми объектами

- Перезаписать все пользовательские объекты из xml-файла
 Заменить все системные объекты на существующие в MaxPatrol

Правила импорта

Выбранные объекты: Создать копию ▾ Перезаписать ▾ Заменить ▾ Не импортировать

Объект	Действие при импорте	Параметры действия
<ul style="list-style-type: none"> ▲ Учетные записи <ul style="list-style-type: none"> Учетная запись «Петров» Учетная запись «Иванов» Учетная запись «SAP*» 	Создать копию с новым названием... ▾ ▾ ▾ Использовать существующий одноименный ▾	Копия УЗ SAP*

XML в MaxPatrol: система отчетности

Формирование XML-отчета

Редактирование отчета

Название

Комментарий

Формат XML file (.xml)

Язык Russian

Тип отчета Информация

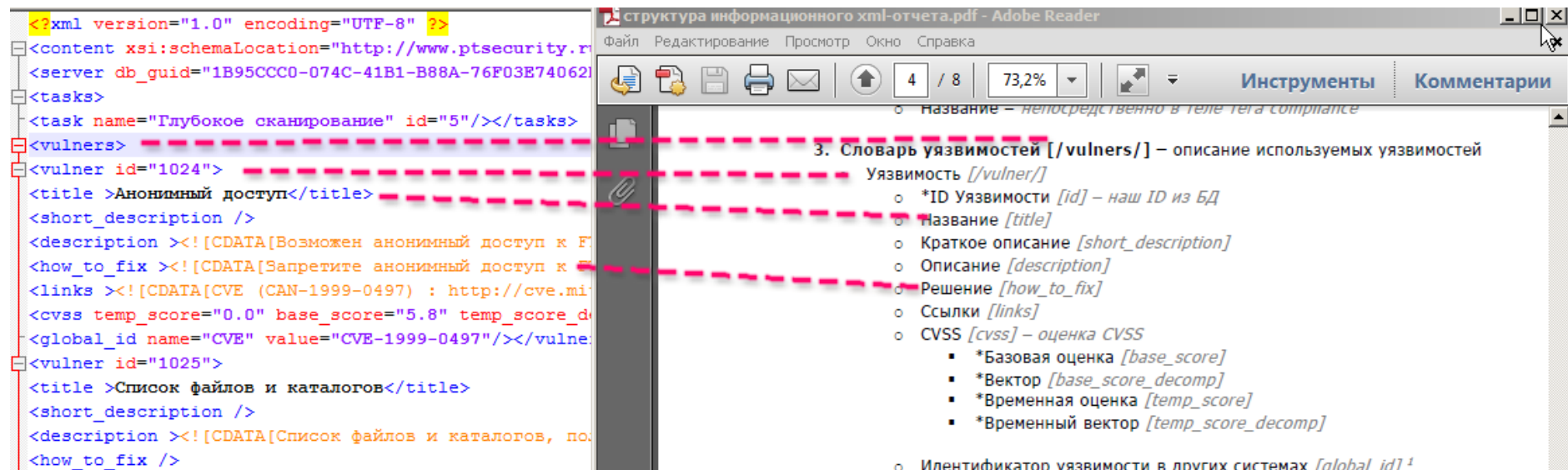
```

<?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



The image shows two windows illustrating the XML report structure. On the left is a code editor displaying XML code for a vulnerability report. On the right is an Adobe Reader window showing the rendered PDF structure of the report.

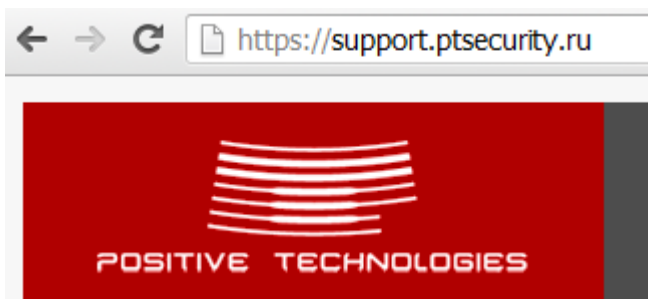
```


<?xml version="1.0" encoding="UTF-8" ?>
<content xsi:schemaLocation="http://www.ptsecurity.ru" ... >
<server db_guid="1B95CCC0-074C-41B1-B88A-76F03E740621" ... >
<tasks>
<task name="Глубокое сканирование" id="5"/></tasks>
<vulners>
<vulner id="1024">
<title>Анонимный доступ</title>
<short_description />
<description ><![CDATA[Возможен анонимный доступ к F...]]>
<how_to_fix ><![CDATA[Запретите анонимный доступ к F...]]>
<links ><![CDATA[CVE (CAN-1999-0497) : http://cve.m...]]>
<cvss temp_score="0.0" base_score="5.8" temp_score_de... >
<global_id name="CVE" value="CVE-1999-0497"/></vulne... >
<vulner id="1025">
<title>Список файлов и каталогов</title>
<short_description />
<description ><![CDATA[Список файлов и каталогов, по...]]>
<how_to_fix />


```

The Adobe Reader window displays the rendered structure of the XML report, showing a section titled "3. Словарь уязвимостей [/vulners/] – описание используемых уязвимостей". The structure includes a list of vulnerabilities with fields for ID, title, short description, description, how to fix, links, CVSS, and global ID.

- 3. Словарь уязвимостей [/vulners/] – описание используемых уязвимостей
 - Уязвимость [/vulner/]
 - *ID Уязвимости [id] – наш ID из БД
 - Название [title]
 - Краткое описание [short_description]
 - Описание [description]
 - Решение [how_to_fix]
 - Ссылки [links]
 - CVSS [cvss] – оценка CVSS
 - *Базовая оценка [base_score]
 - *Вектор [base_score_decomp]
 - *Временная оценка [temp_score]
 - *Временный вектор [temp_score_decomp]
 - Идентификатор уязвимости в других системах [global id]¹

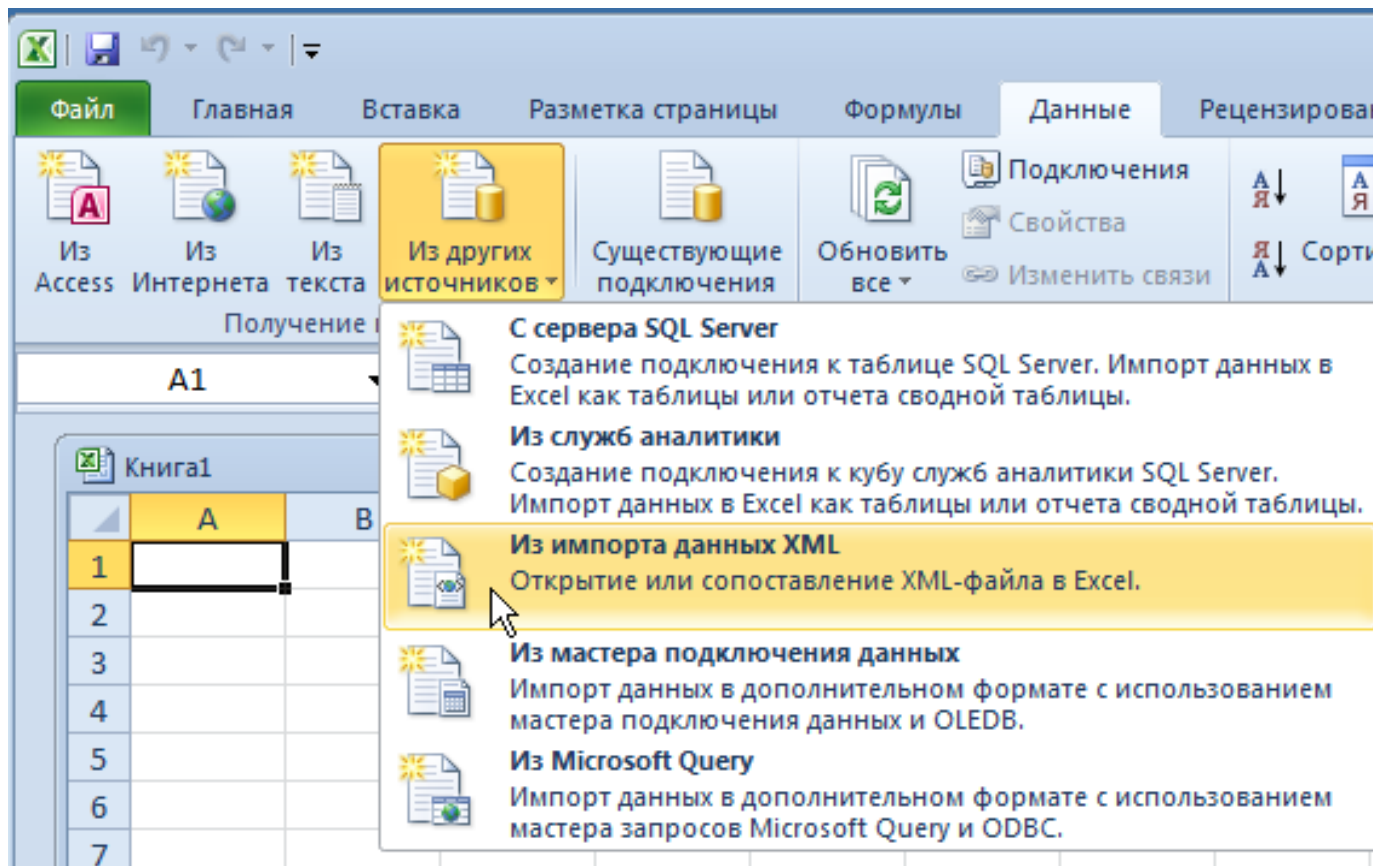


 Структура дифференциального XML-отчета
Во вложении.

 Структура информационного XML-отчета
Во вложении.

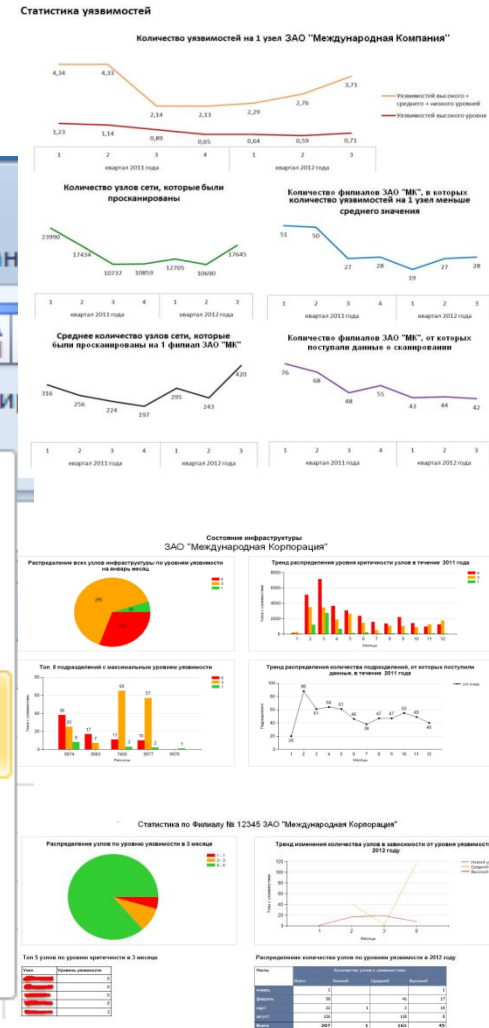
XML в MaxPatrol: система отчетности

Обработка XML-отчета в Excel



The screenshot shows the Microsoft Excel interface with the 'Данные' (Data) ribbon selected. The 'Из других источников' (From other sources) dropdown menu is open, displaying several options for data import:

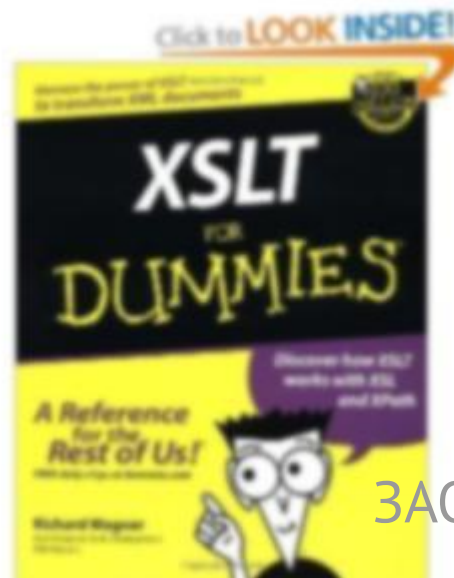
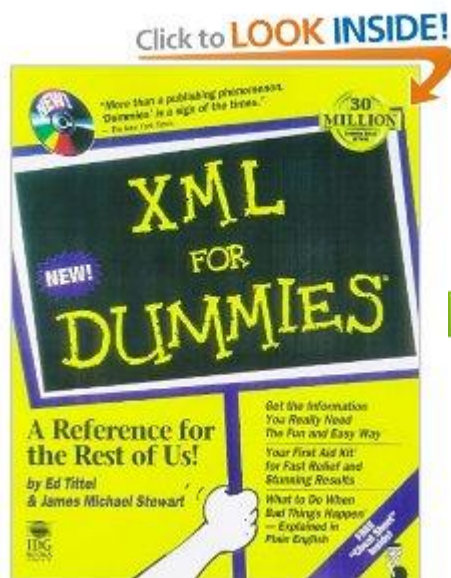
- Из других источников** (From other sources)
- С сервера SQL Server** (From SQL Server server): Создание подключения к таблице SQL Server. Импорт данных в Excel как таблицы или отчета сводной таблицы.
- Из служб аналитики** (From analytics services): Создание подключения к кубу служб аналитики SQL Server. Импорт данных в Excel как таблицы или отчета сводной таблицы.
- Из импорта данных XML** (From XML data import): Открытие или сопоставление XML-файла в Excel. (This option is highlighted with a mouse cursor)
- Из мастера подключения данных** (From data connection wizard): Импорт данных в дополнительном формате с использованием мастера подключения данных и OLEDB.
- Из Microsoft Query** (From Microsoft Query): Импорт данных в дополнительном формате с использованием мастера запросов Microsoft Query и ODBC.



Часть 2.

XML для «чайников»

Гроссмейстер пошел e2-e4



Павел Лысов

старший программист

ЗАО «Positive Technologies»

МНТ/PDF кому мало?



МНТ
веб-архив



PDF



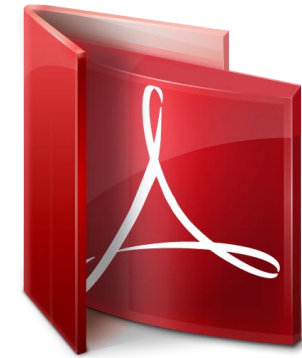
MHT/PDF кому мало?



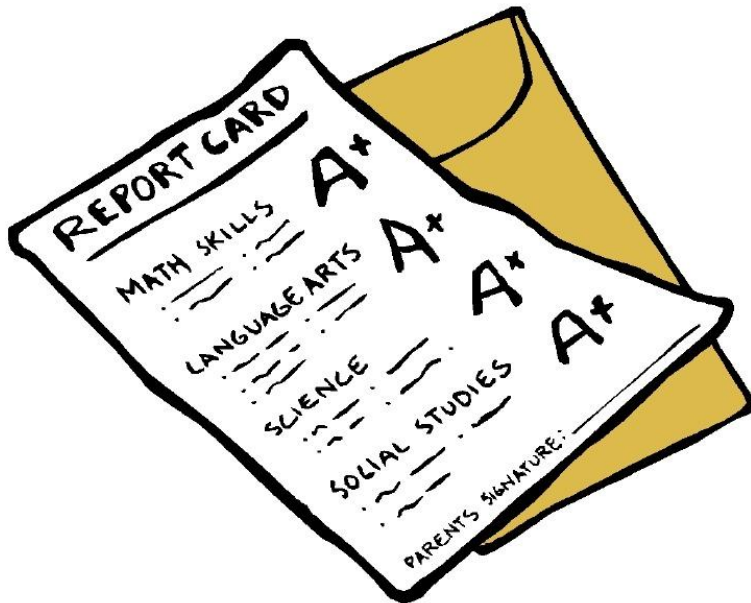
MHT
веб-архив



PDF



Плюсы и минусы, а есть ли они?



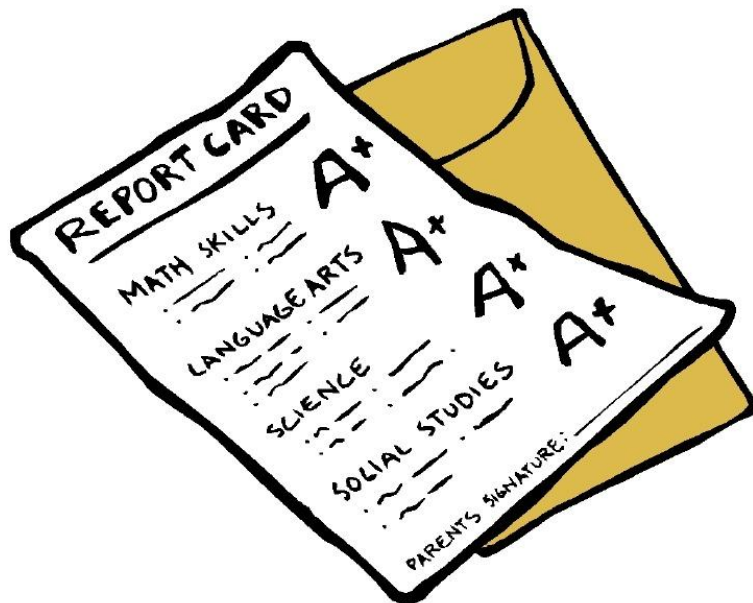
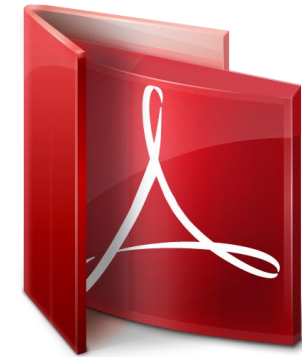
MHT/PDF кому мало?



MHT
веб-архив



PDF



Плюсы и минусы, а есть ли они?

“**плюсы**”:

- это красиво =)

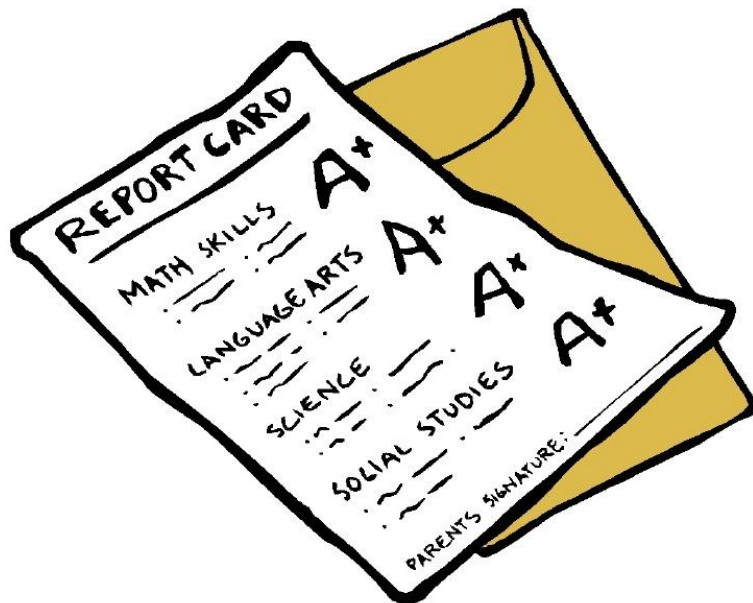
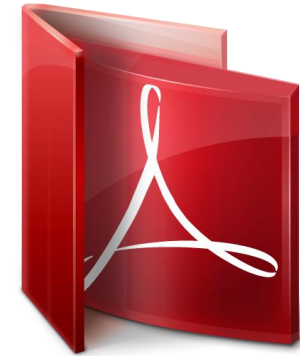
MHT/PDF кому мало?



MHT
веб-архив



PDF



Плюсы и минусы, а есть ли они?

“**плюсы**”:

- это красиво =)
- вариант из коробки

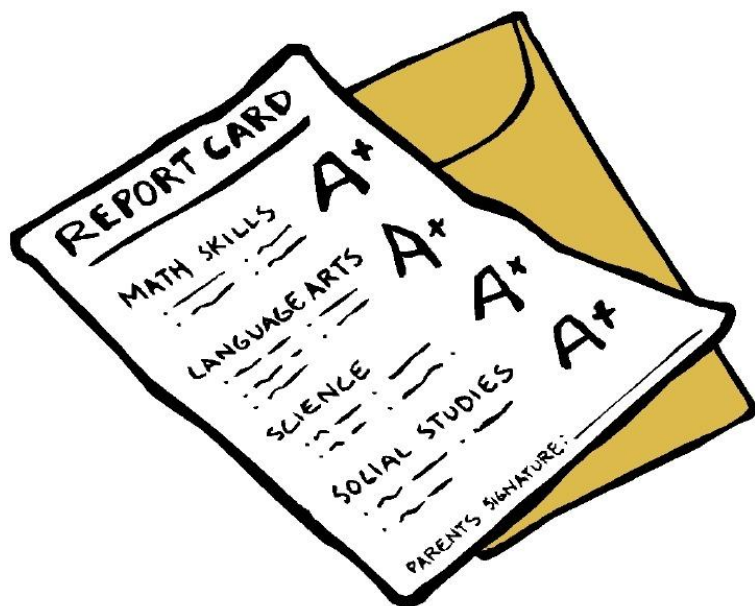
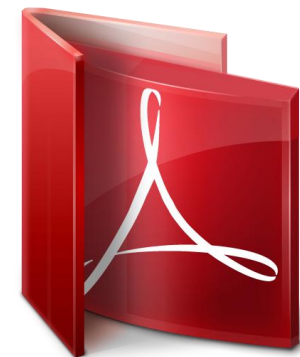
MHT/PDF кому мало?



MHT
веб-архив



PDF



Плюсы и минусы, а есть ли они?

“**плюсы**”:

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

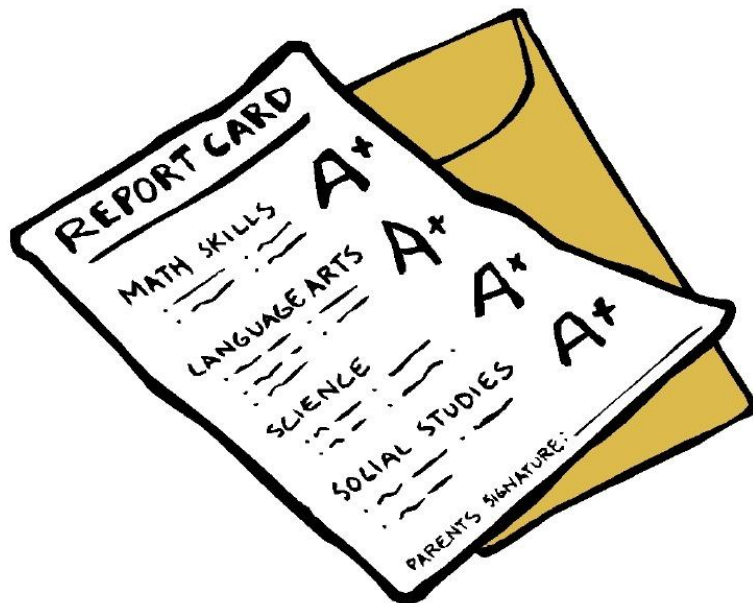
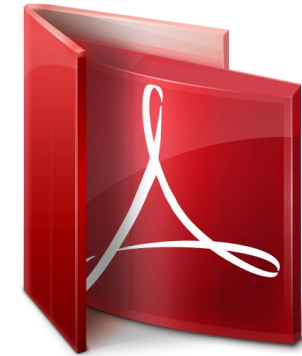
MHT/PDF кому мало?



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

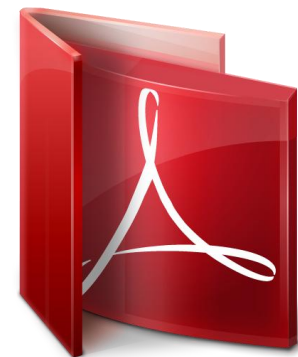
МНТ/PDF кому мало?



МНТ
веб-архив



PDF



А что по поводу минусов?



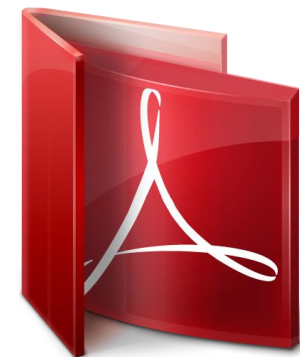
MHT/PDF кому мало?



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



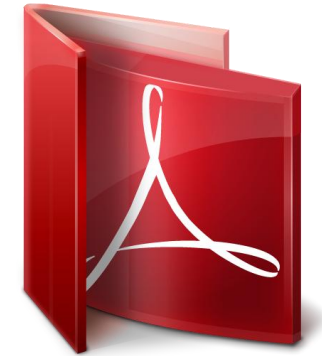
МНТ/PDF кому мало?



МНТ
веб-архив



PDF



А что по поводу минусов?

“**МИНУСЫ**”:

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



XML, альтернатива ли?



XML-отчет противоположность МНТ/PDF:

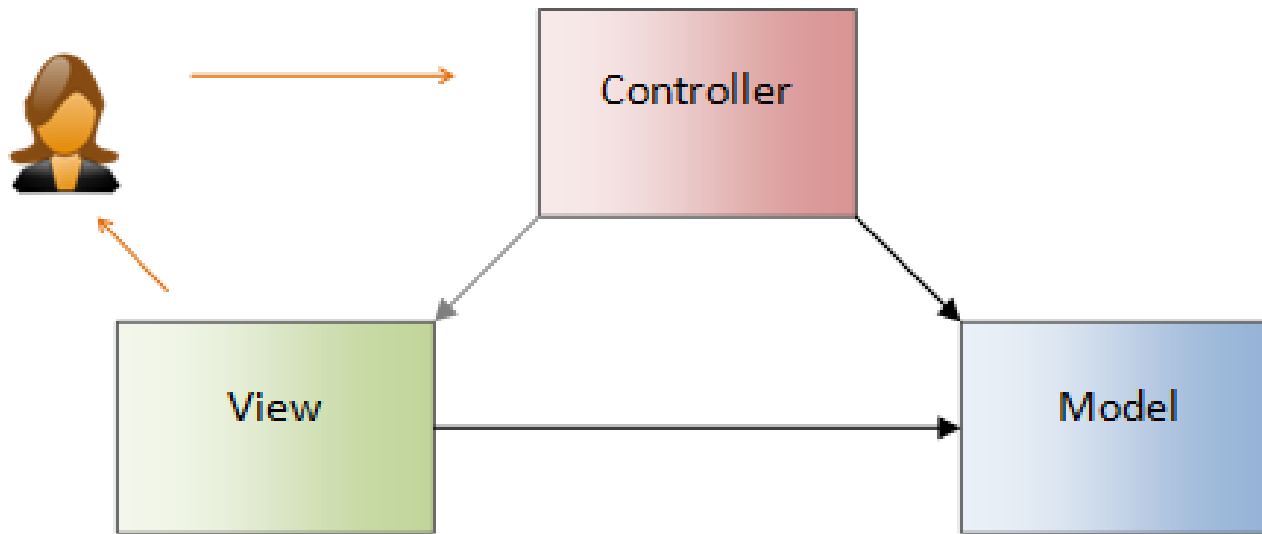
```
<?xml version="1.0" encoding="UTF-8" ?>
- <content xsi:schemaLocation="http://www.ptsecurity.ru/reports
  https://support.ptsecurity.ru/xsd/mp8/24/maxpatrol80-info-report.xsd"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns="http://www.ptsecurity.ru/reports"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">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

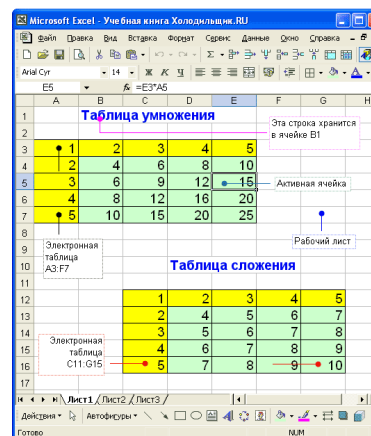
Представление XML, как использовать?

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

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



— Excel — как инструмент работы с таблицами

	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

	1	2	3	4	5
1	1	2	3	4	5
2	2	4	5	6	7
3	3	5	6	7	8
4	4	6	7	8	9
5	5	7	8	9	10



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.)



Microsoft®
SQL Server® 2008 R2

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

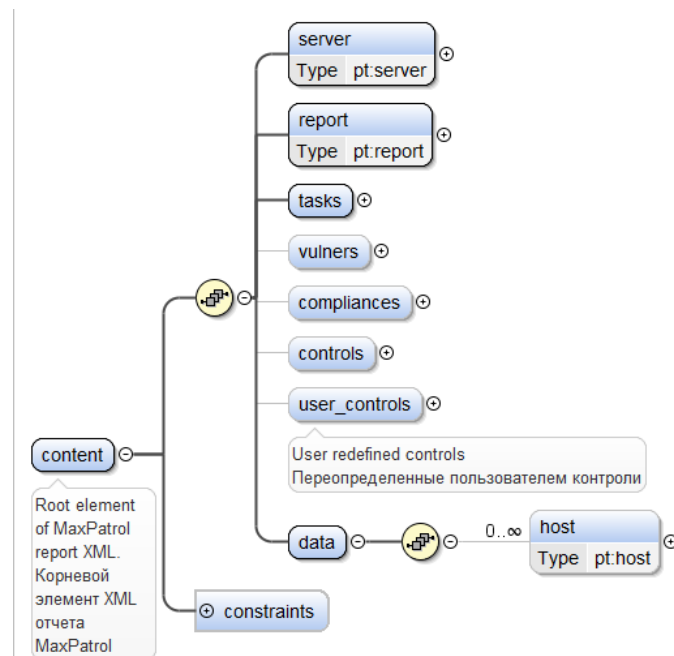
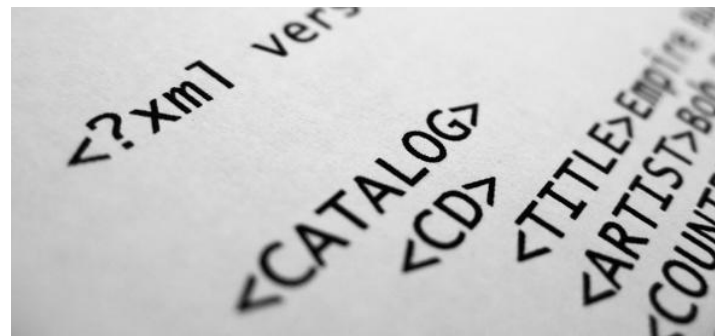


crystal reports®



Excel для представления XML отчетов?

- Импорт RAW данных из XML
- Карта XML, она же схема XSD



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:

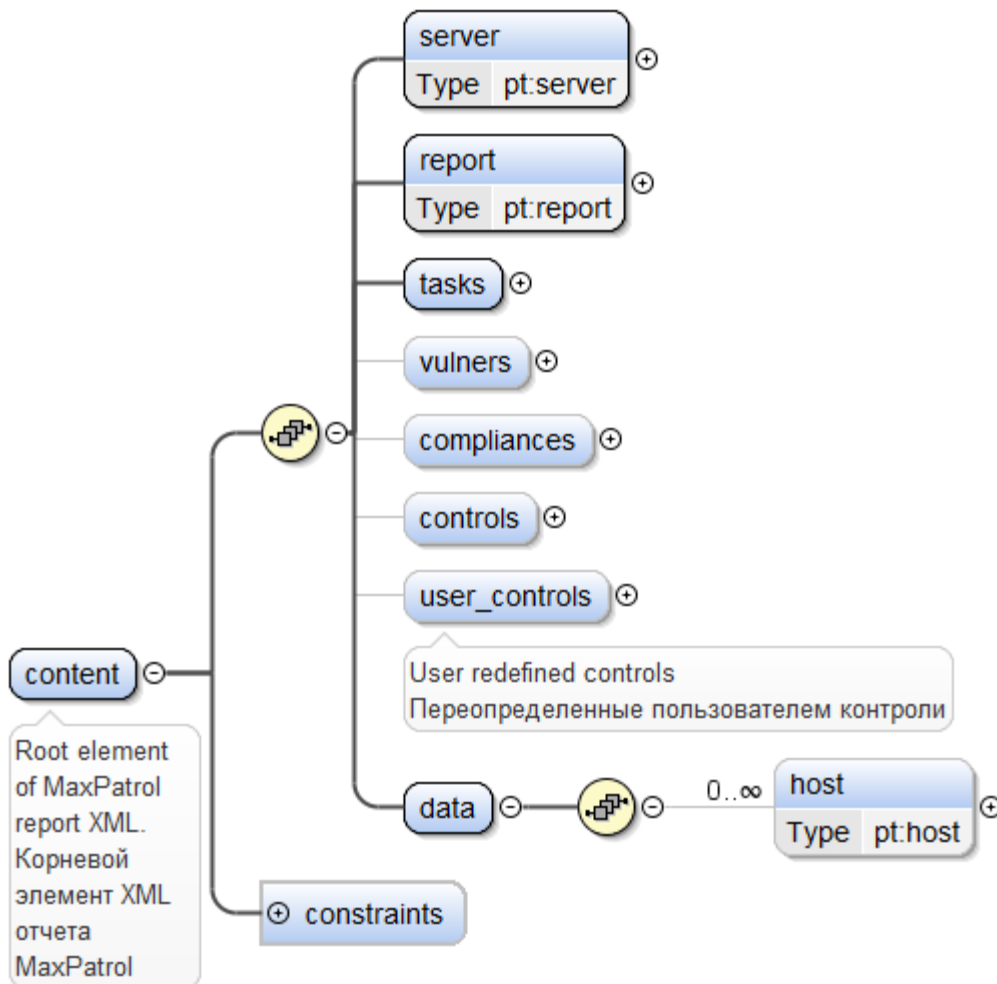
```
<?xml version="1.0" encoding="UTF-8" ?>  
- <content xsi:schemaLocation="http://www.ptsecurity.ru/reports  
  https://support.ptsecurity.ru/xsd/mp8/24/maxpatrol80-info-report.xsd"  
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"  
  xmlns="http://www.ptsecurity.ru/reports"  
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">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

— Локально из консоли MaxPatrol



Импорт XML с картой

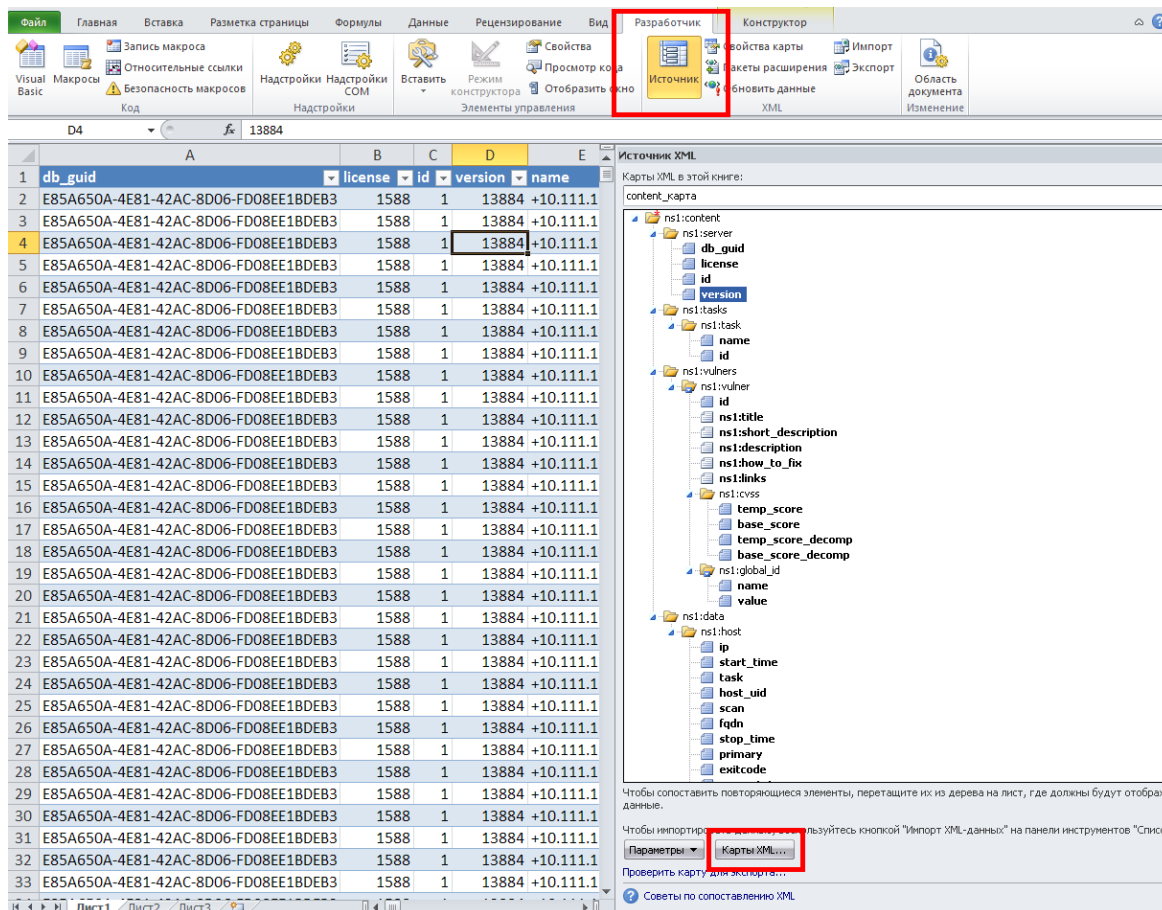
Берегите пенсне, Киса! Сейчас начнется!



Импорт XML с картой

Берегите пенсне, Киса! Сейчас начнется!

— Как воспользоваться картой XML в Excel?

The screenshot shows the Excel interface with the 'Источники' (Sources) task pane open on the right. The 'Источники XML' (XML Sources) section is active, showing a tree view of the XML data. The 'content_карта' (content_map) folder is expanded, revealing a table of data. The table has columns for 'db_guid', 'license', 'id', 'version', and 'name'. The 'version' column contains the value '13884' in row 4, which is highlighted in the original image. Below the table, there are instructions in Russian: 'Чтобы сопоставить повторяющиеся элементы, перетащите их из дерева на лист, где должны будут отображаться данные.' and 'Чтобы импортировать данные из XML-карты, используйте кнопку "Импорт XML-данные" на панели инструментов "Список"'. The 'Импорт XML-данные' button is highlighted with a red box in the original image.

	A	B	C	D	E
	db_guid	license	id	version	name
1	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
2	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
3	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
4	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
5	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
6	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
7	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
8	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
9	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
10	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
11	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
12	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
13	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
14	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
15	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
16	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
17	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
18	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
19	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
20	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
21	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
22	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
23	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
24	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
25	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
26	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
27	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
28	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
29	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
30	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
31	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
32	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1
33	E85A650A-4E81-42AC-8D06-FD08EE1BDEB3	1588	1	13884	+10.111.1

Примеры Excel отчетов

- Отчет по Active Directory
- Дифференциальный отчет
- Сводный отчет по Compliance

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	
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	
По всем узлам		Узлов: 2	всего	4	6	10	32
			всего без подозрений	4	6	10	32

A	B
Имя домена	mscorp
Имя группы	Developers
Название организационной единицы	Имя доменного контроллера
	Имя доменного контроллера
	Maxim Shchegolev
	Victor Shchegolev
	Konstantin Kozlovich
	Vladimir Shchegolev
	Anton Shchegolev
	Yury Kozlov
	Pavel Morozov

Итоги. Части 2.

Использование формата XML позволило решить проблемы:

- Интеграции
- Редактируемого формата

Остались проблемы:

- Отсутствие гибкости
- Большой размер отчета



Часть 3. X-MAN

Командовать парадом буду я!



Павел Лысов

старший программист
ЗАО «Positive Technologies»

Использование XSLT и XPath.

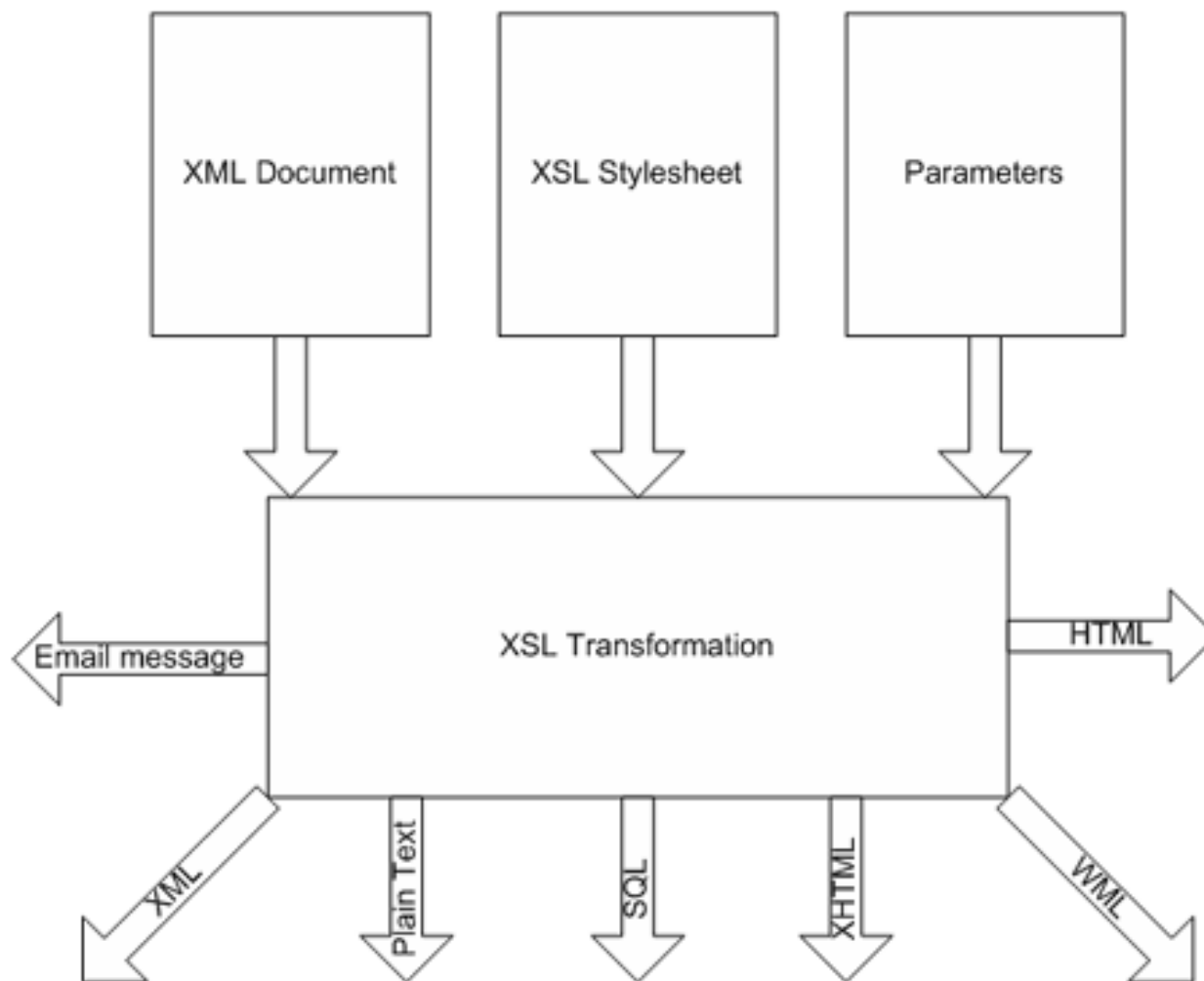
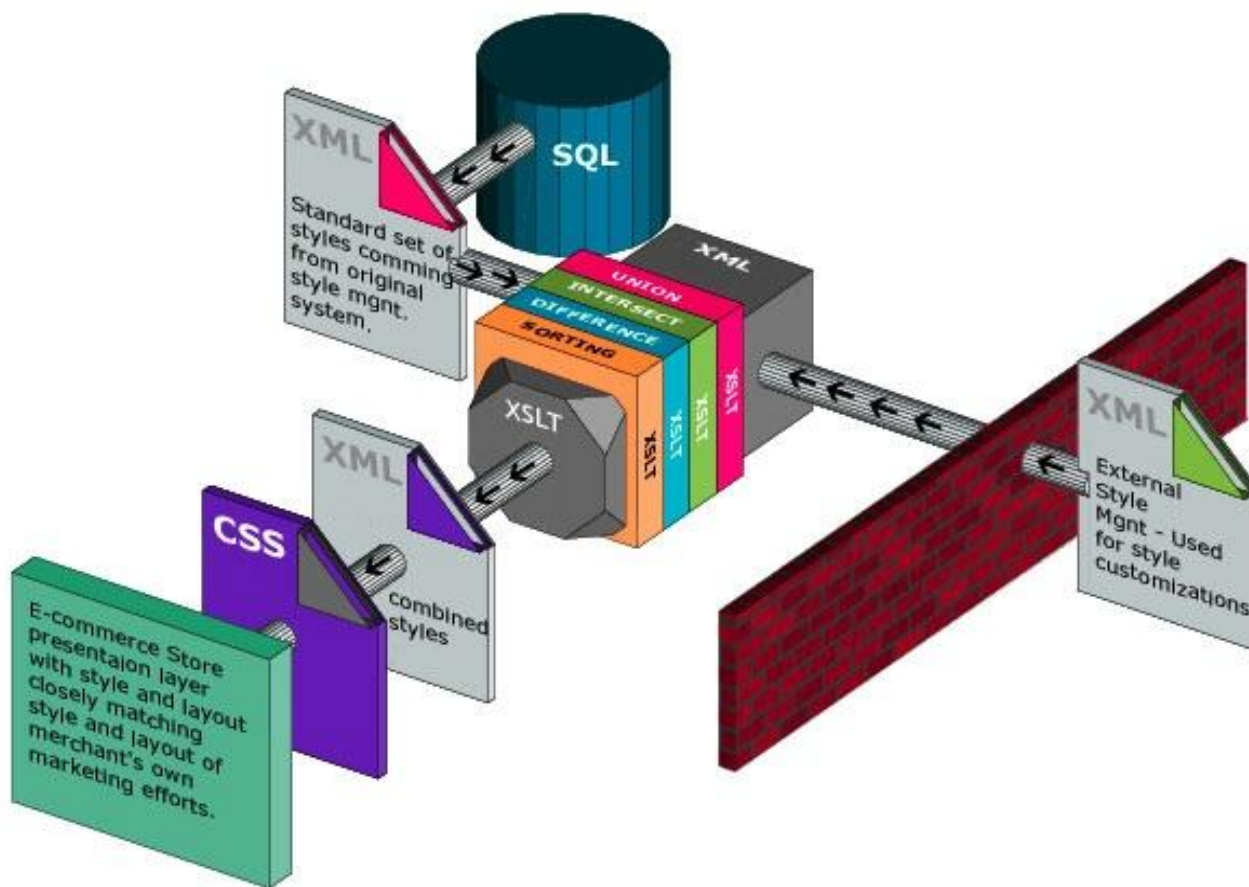


Схема работы генератора отчета в формате XML MaxPatrol 8.0 с использованием XSLT шаблона



Как применить XSLT в MaxPatrol?

Редактирование отчета

Название: Состав пользователей, входящих в указанную группу

Комментарий

Формат: XML file (.xml) Шаблон: **Active Directory - List of users in the group**

Язык: English Добавлять BOM

Тип отчета

Информация Сравнительный аналитический
 Дифференциальный Динамический аналитический
 Аналитический

Исходные данные

По скану По задаче/задачам

Тип данных

PenTest Audit Compliance Forensic

Выбор задачи и скана

Задача: task Скан: 06.09.2012 16:33:30 /завершен/

Данные для XML-отчета

Доменные группы: Доменные группы

Фильтр узлов

Достоверность результатов: любая (все результаты)
Включать узлы, отмеченные как: <Все>
 Включать узлы, сканирование которых завершено с ошибкой
 Включать узлы, данные о которых отсутствуют
Дополнительный: <не установлен>

Фильтр данных

Не использовать
 По уровню
 По группе: <не установлено>
 По полю

Фильтр программного обеспечения

Не использовать
<Не выбрано>

Сохранить как... Сохранить Отмена

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			
22	<p><i>Positive Technologies</i> 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. <i>Positive Technologies</i> 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.</p>			
23				
24	ASV Attestation			
	<p>This scan and report was prepared and conducted by <i>Positive Technologies</i> under certificate number 1, according to internal processes that meet PCI DSS requirement 11.2 and the PCI DSS ASV Program Guide. <i>Positive Technologies</i> 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 <i>Dmitry Evteev</i>.</p>			



Итоги. Части 3.

Использование формата XML + XSLT позволило решить проблемы:

- Интеграции
- Редактируемого формата
- Гибкость
- Большой размер отчета



Часть 4. Reporting Services

Заседание продолжается!



Павел Лысов

старший программист
ЗАО «Positive Technologies»

В чем соль?



В чем соль?

- Работа с большими объемами данных



В чем соль?

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



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



В чем соль?

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



Как это работает?



Как это работает?

- Производится сканирование MaxPatrol

Как это работает?

- Производится сканирование MaxPatrol
- Выпускается отчетность в формате XML

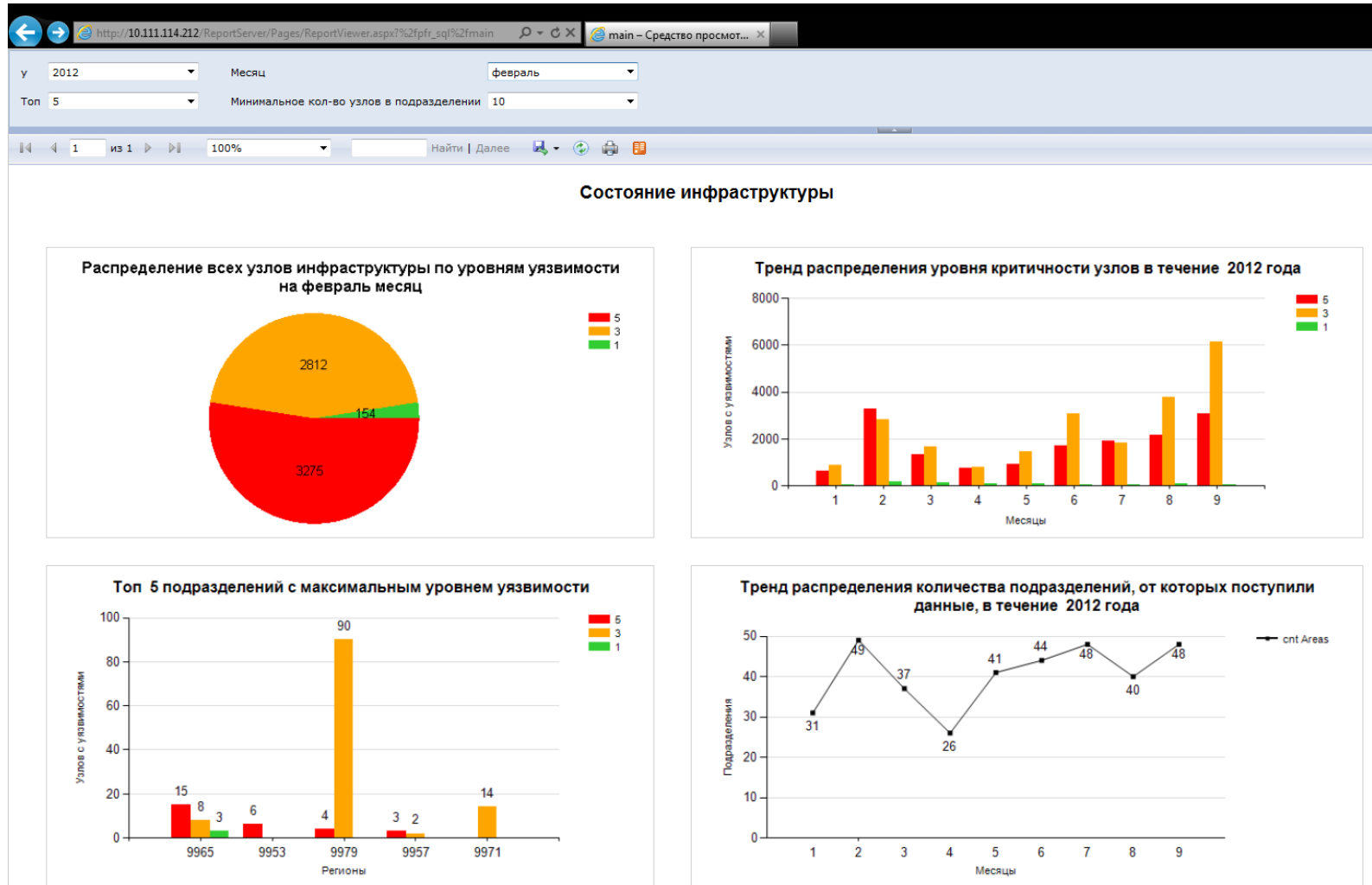
Как это работает?

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

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.



Конец рассказа

Спасибо за внимание

Александр Веретенников

averetennikov@ptsecurity.ru

Павел Лысов

plysov@ptsecurity.ru