Возможности по интеграции в MaxPatrol

Олег Матыков

Руководитель отдела проектных решений

POSITIVE TECHNOLOGIES

ОБЗОР ВОЗМОЖНОСТЕЙ ИНТЕГРАЦИИ С MAXPATROL

Возможные цели интеграции. Экспорт и преобразование данных.

- **Передача данных об уязвимостях на узлах. Например, для снижения количества ложных срабатываний в SIEM**
- **Передача данных об обнаруженных узлах и инвентарной информации. Например, для в базу данных управления конфигурациями**
- **Передача данных по изменениям в инфраструктуре ИТ, настройках и уровня защищенности информационных систем. Например, для передачи в систему управления инцидентами или управления ИТ**

Возможные цели интеграции. Импорт данных.

- **Импорт из каталога Active Directory. Синхронизация по расписанию узлов задачи с узлами в указанном контейнере.**
- **Импорт по расписанию настроек MaxPatrol, например, сформированных сторонним приложением.**
- **Управление параметрами сканирования MaxPatrol, с использованием сторонних приложений**

Механизм интеграции

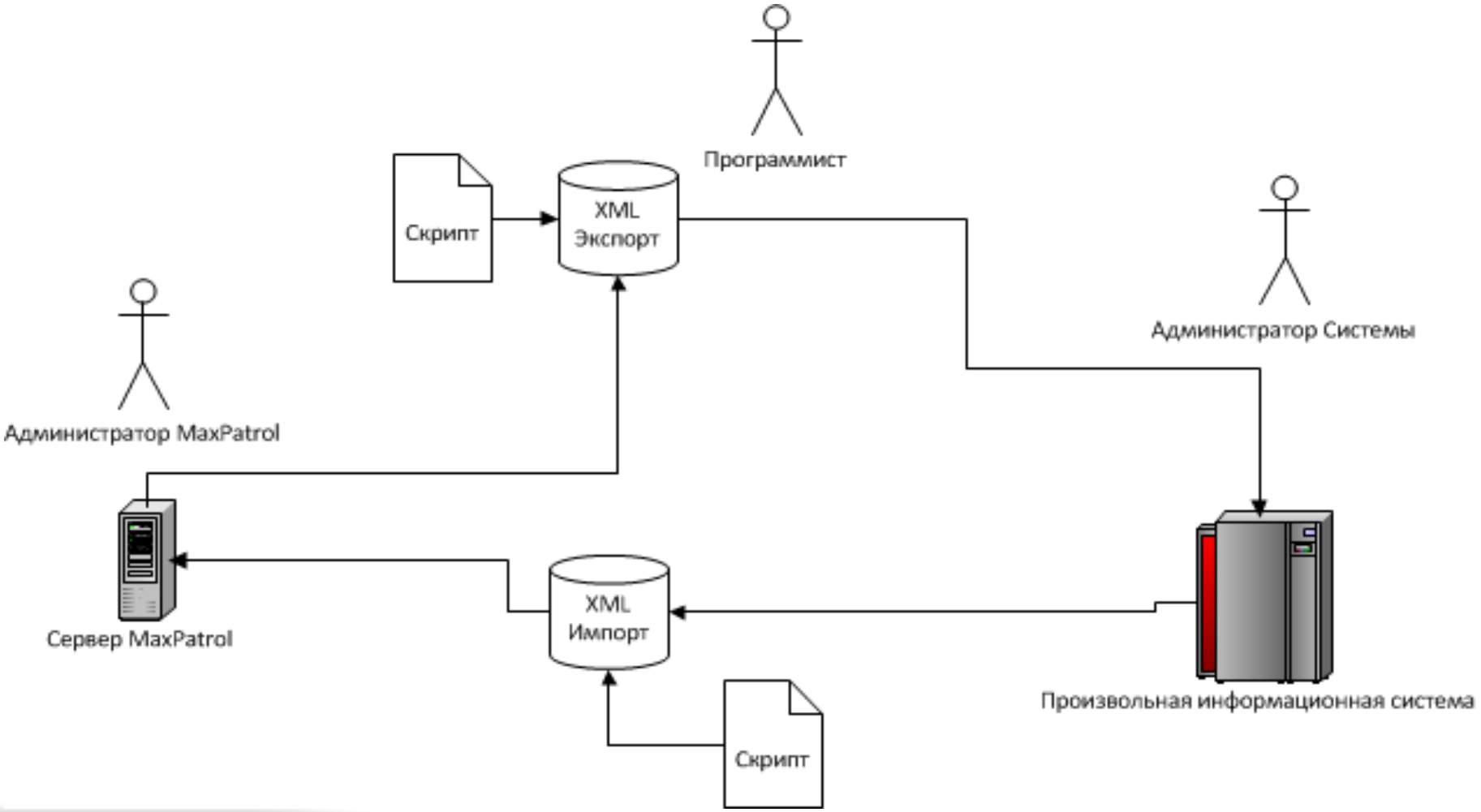
Использование XML – основной механизм интеграции MaxPatrol.

Основные возможности:

- **Экспорт отчётов с данными по сканированию в ручном и автоматическом режиме в файловый каталог или почтовый ящик. Для экспорта доступна практически вся информация о сканировании.**
- **Экспорт и импорт настроек MaxPatrol через файловый каталог.**

КОНЦЕПЦИЯ ИНТЕГРАЦИИ С ПРОИЗВОЛЬНОЙ СИСТЕМОЙ

Концепция интеграции с произвольной системой



Импорт настроек MaxPatrol из произвольной системы

Цель: Управления заданиями на сканирование, обновление данных

В текущей версии можно импортировать:

- **Расписания**
- **Задачи**
- **Профили и их переопределения**
- **Справочники**
- **Переопределения стандартов**
- **Учётные записи (без пароля)**

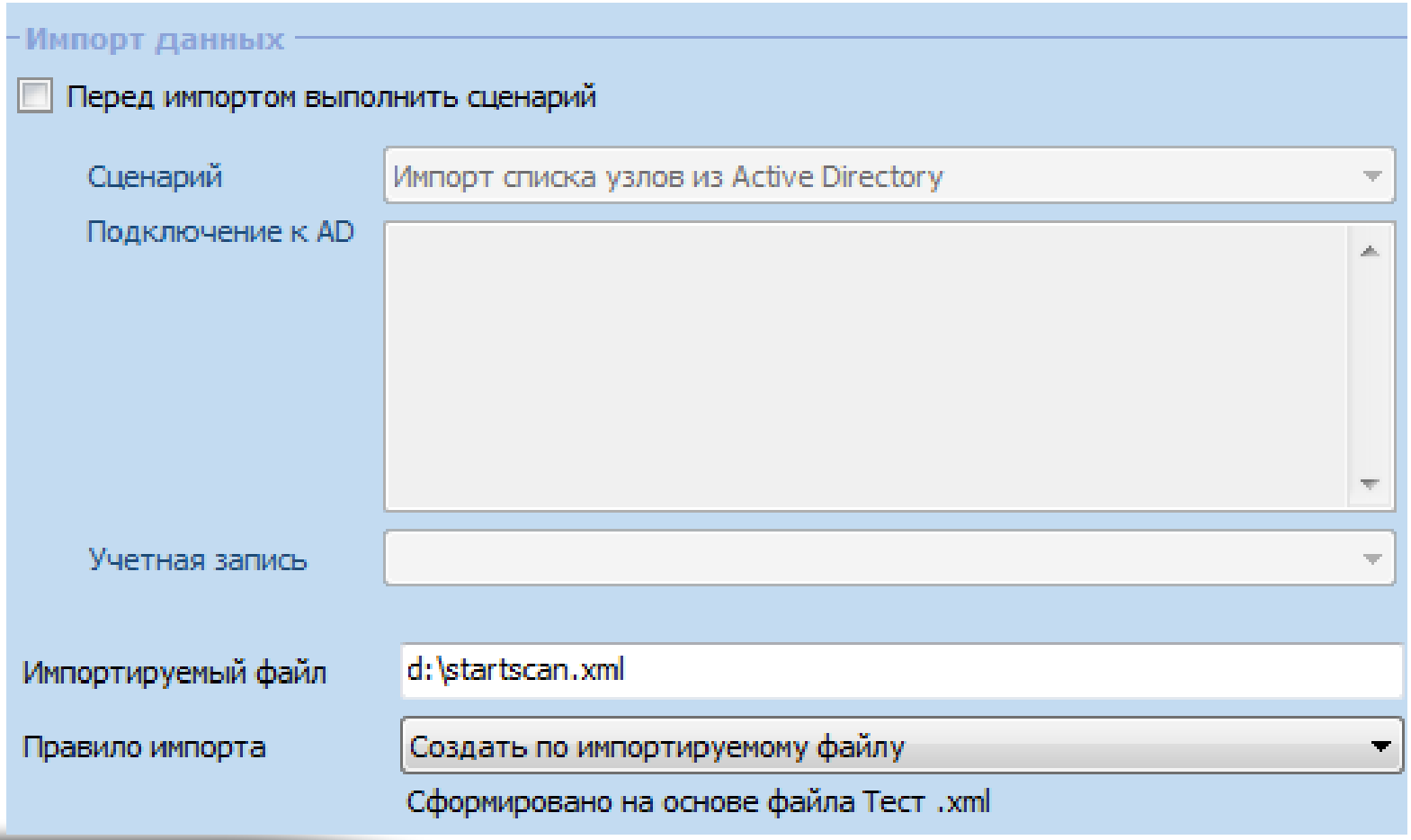
Импорт настроек MaxPatrol из произвольной системы

Порядок настройки:

1. **Выбрать и экспортировать объекты импорта**
2. **Настроить расписание по импорту данных**
3. **Настроить пользовательское приложение или скрипт таким образом, чтобы в импортируемый файл xml вносились необходимые изменения до начала импорта по расписанию**

Импорт настроек MaxPatrol из произвольной системы

Пример настройки расписания:



Импорт настроек MaxPatrol из произвольной системы

Справочник паролей:

```
<?xml version="1.0" encoding="utf-8"?>
<Package xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xsi:schemaLo
xmlns="http://www.ptsecurity.ru/import">
    <schedules />
    <dictionaries>
        <dictionary id="10" name="rdp-passwords" type="1">qwerty
qwerty123
test
admin
1
123
123456
12345678
P@ssw0rd
q1
q1q1
q1q1q1
1234
1234567890
123456789
azerty
password
password1</dictionary>
    </dictionaries>
    <accounts />
    <profiles />
    <complianceSettings />
    <tasks />
    <qrules />
</Package>
```

Импорт настроек MaxPatrol из произвольной системы

Время запуска сканирования:

```
<?xml version="1.0" encoding="UTF-8"?>
<Package xmlns="http://www.ptsecurity.ru/import" xsi:schemaLocation="http://www.ptsecurity.ru/import https://support.pt
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  - <schedules>
      - <schedule force_run="0" frozen="0" scenario="3" name="Тест " Guid="56dd545d-a47f-4807-b2cb-309db36b9991" task_sta
            <schedule_reports/>
          - <schedule_params>
                <schedule_param Type="1" StringValue="" DwordValue="18" ImportToolType="0" FileTypeValue="0" BreakStrategyValue
                <schedule_param Type="2" StringValue="" DwordValue="86400" ImportToolType="0" FileTypeValue="0" BreakStrategyV
                <schedule_param Type="3" StringValue="" DwordValue="172800" ImportToolType="0" FileTypeValue="0" BreakStrategy
                <schedule_param Type="5" StringValue="" DwordValue="1000000" ImportToolType="0" FileTypeValue="0" BreakStrate
                <schedule_param Type="7" StringValue="" DwordValue="0" ImportToolType="0" FileTypeValue="0" BreakStrategyValue=
            </schedule_params>
          - <schedule_timers>
                <schedule_timer param2="0" param1="1" stop_time="2037-01-18T23:59:59" start_time="2011-04-26T09:54:00" ti
                <schedule_timer param2="31457400" param1="1" stop_time="2037-01-18T23:59:59" start_time="2011-04-26T09:
```

POSITIVE TECHNOLOGIES

Экспорт данных MaxPatrol в произвольную систему

Цель: Передача результатов сканирования в произвольную систему

В текущей версии можно выгружать следующую информацию:

- **Обнаруженные уязвимости в режимах Pentest и Audit**
- **Обнаруженные узлы и операционные системы**
- **Установленные приложения и аппаратное обеспечение**
- **Результат проверки соответствию техническим требованиям**
- **Обнаруженные изменения между двумя сканированиями**

Экспорт данных MaxPatrol в произвольную систему

Перед загрузкой данных из MaxPatrol в произвольную систему может потребоваться предварительная обработка XML

Для преобразования XML отчётов MaxPatrol можно, например, использовать XSLT или макрос на языке VBA

Экспорт данных MaxPatrol в произвольную систему

Порядок настройки:

1. **Настроить отчёт MaxPatrol в формате XML с необходимым набором данных**
2. **Настроить доставку XML файла в нужный файловый каталог и настроить расписание по доставке нужного отчёта**
3. **При необходимости запустить скрипт по преобразованию отчёта**
4. **Импортировать данные с использованием механизмов произвольного приложения**

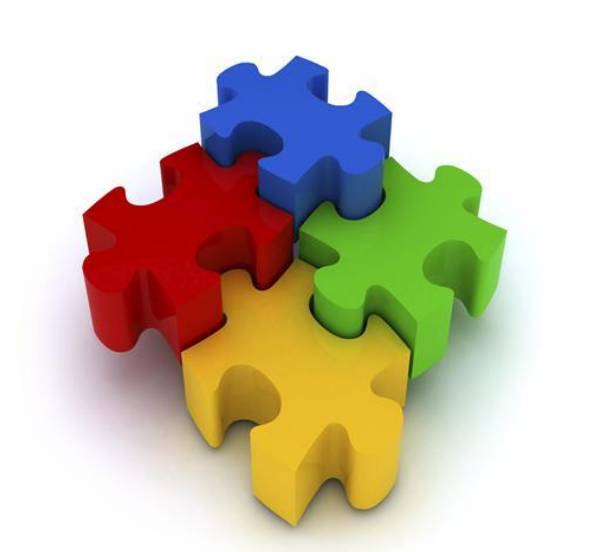
Основная проблема интеграции

В текущей версии MaxPatrol предусмотрены механизмы импорта и экспорта, но для полноценной интеграции часто требуется разработка скриптов для преобразования данных перед импортом или экспортом

Примеры некоторых скриптов можно получить по запросу:

- импорт списка баз из Oracle и MS SQL
- Несколько примеров xslt для форматирования результатов сканирования

ИНТЕГРАЦИЯ С ACTIVE DIRECTORY



Интеграция с Active Directory

Цель: Однократная или периодическая синхронизация узлов в задаче с указанным контейнером каталога

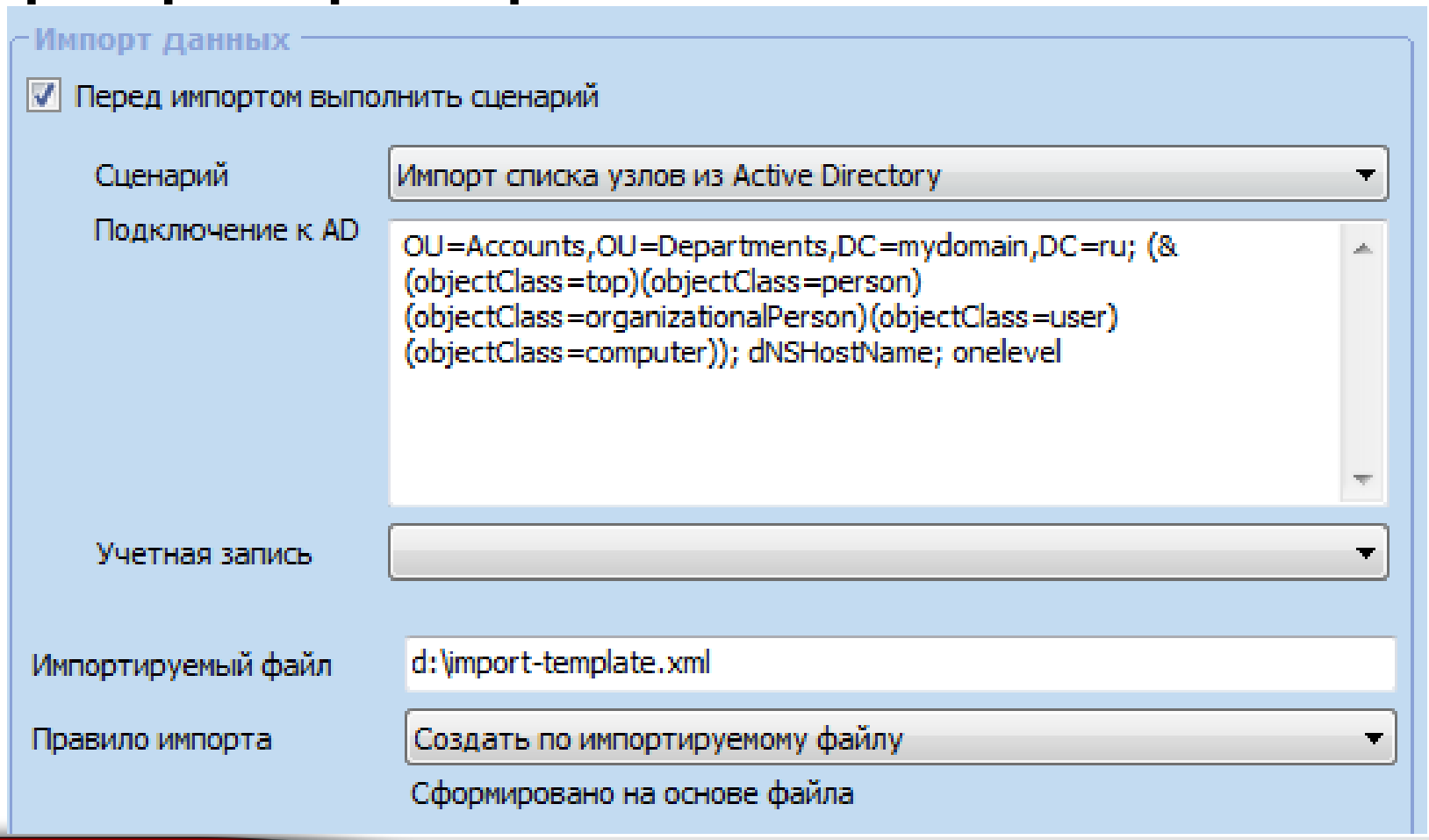
Порядок настройки:

1. **Настройка расписания по импорту данных. Нужно указать: путь к контейнеру, учётную запись для подключения к AD, путь к импортируемому файлу и правила импорта.**

2. **Запустить расписание. Будет создана задача с узлами из указанного контейнера**

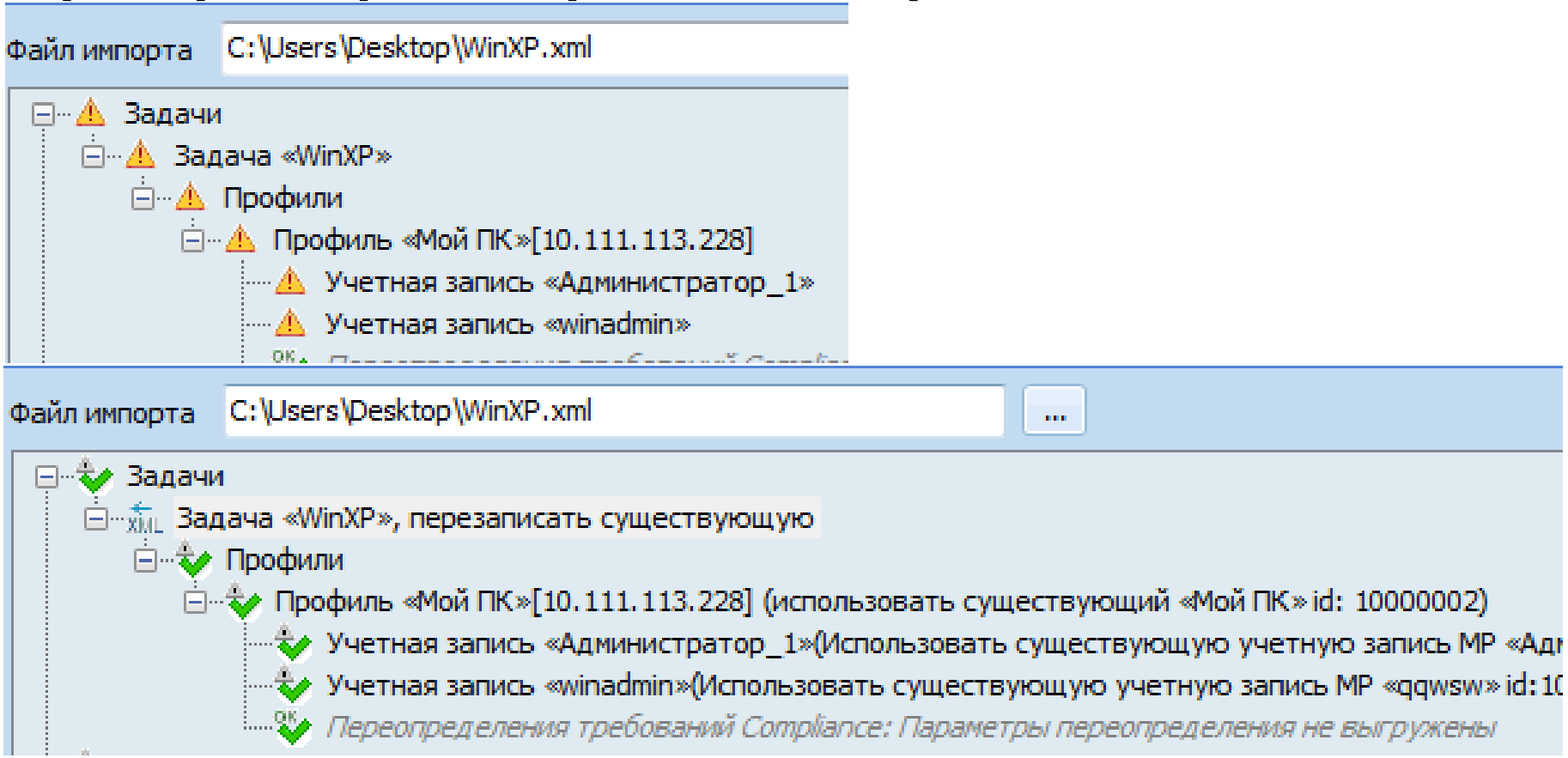
Интеграция с Active Directory

Пример настройки расписания:



Интеграция с Active Directory

Пример настройки правила импорта:



Спасибо за внимание!

Олег Матыков omatykov@ptsecurity.ru

Тел. (495) 744-01-44

POSITIVE TECHNOLOGIES

MAXPATROL

Возможности интеграции MaxPatrol с SIEM и RMIS

Евгения Поцелуевская, CISA, CISSP

ведущий консультант Positive Technologies

epotseluevskaya@ptsecurity.ru

POSITIVE TECHNOLOGIES

Системы типа SIEM и RMIS

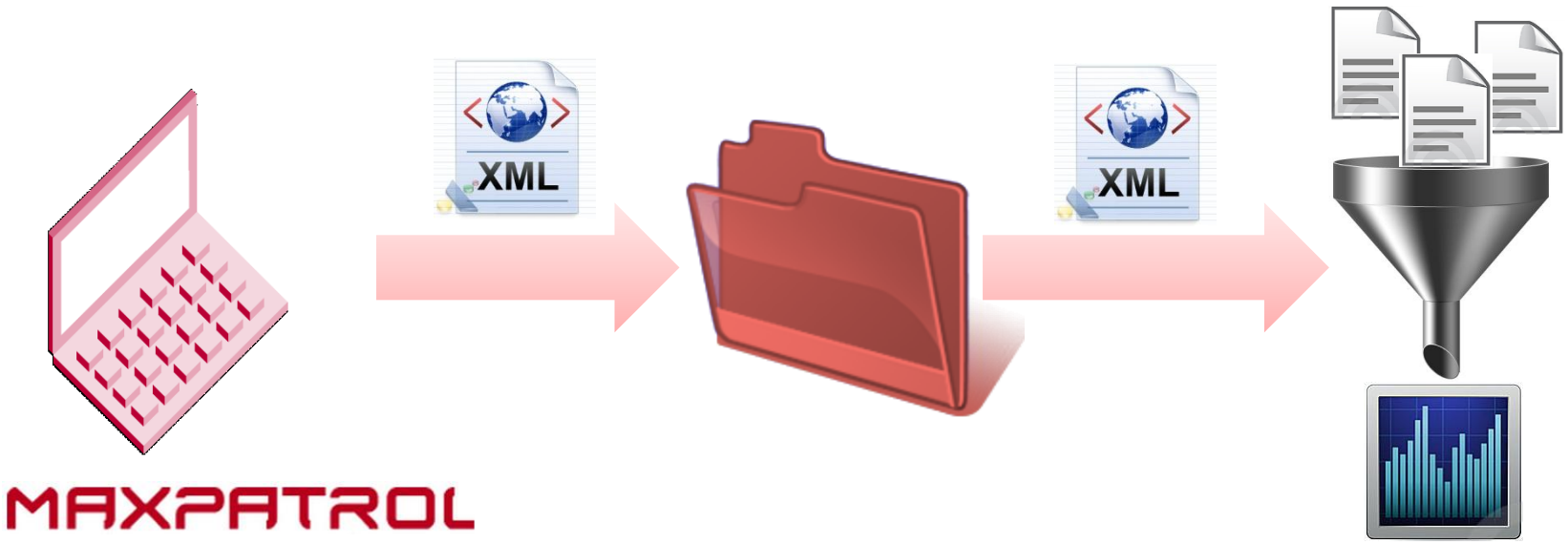
- **Системы сбора и управления событиями информационной безопасности (Security Incident and Event Management, SIEM)** предназначены для централизованного сбора, хранения, анализа и корреляции событий безопасности, поступающих от различных источников

- **Системы управления рисками (Risk Management Information System, RMIS)** предназначены для вычисления степени угрозы информационным активам предприятия в режиме реального времени

Цели интеграции с SIEM и RMIS

- **Инвентаризация узлов сети (в том числе формирование модели сети)**
- **Снижение вероятности ложных срабатываний при обработке событий от систем обнаружения вторжений**
- **Более точная оценка рисков для активов в соответствии с актуальной информацией об уязвимостях**
- **Оперативный централизованный контроль результатов сканирования, поступающих от MaxPatrol**

Схема интеграции с SIEM и RMIS



Системы, интегрируемые с MaxPatrol

SIEM-системы:

- **ArcSight ESM**
- **Symantec SIM**
- **Cisco MARS**

RMIS-система:

- **Skybox View**

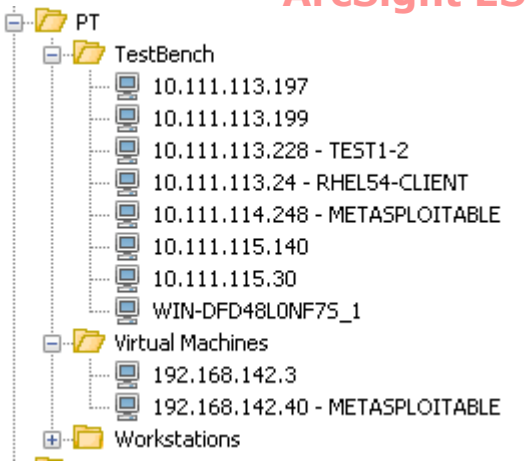
Основная информация для экспорта

Перечень узлов

IP Address	Host Name	Vulnerable
10.111.112.50	rosb.ptsecurity.ru	Yes
10.111.113.24	rhel54-client	Yes
10.111.113.100	win7xsp1t-pc	Yes
10.111.113.103	wmi-du	Yes
10.111.113.195	10.111.113.195	Yes
10.111.113.197	10.111.113.197	Yes
10.111.113.228	test1-2	Yes
10.111.114.194	qualys	

Symantec SIM

ArcSight ESM



Name	Primary IP Address
RHEL54-CLIENT	10.111.113.24
10.111.113.197	10.111.113.197
10.111.113.199	10.111.113.199
TEST1-2	

Skybox View

Name	IP Address
H-10.111.113.1	10.111.113.1
H-10.111.113.10	10.111.113.10
H-10.111.113.197	10.111.113.197
H-10.111.113.199	10.111.113.199
H-10.111.113.2	10.111.113.2
H-10.111.113.3	10.111.113.3
H-10.111.113.4	10.111.113.4

Cisco MARS

Основная информация для экспорта

Перечень уязвимостей

ArcSight ESM

Radar

Scan Date	Severity	Vulnerability	Name
9 авг 2011 11:57:34 MSD	5	MaxPatrol - 412410	MS Paint Integer Overflow Vulnerability
26 авг 2011 15:19:11 MSD	3	MaxPatrol - 10008	Антивирусные базы устарели
9 авг 2011 11:57:34 MSD	3	MaxPatrol - 10008	Антивирусные базы устарели
9 авг 2011 11:57:34 MSD	5	MaxPatrol - 171625	Внедрение XML-кода
9 авг 2011 11:57:34 MSD	5	CVE - CVE-2008-5024	Внедрение XML-кода
26 авг 2011 15:19:11 MSD	5	MaxPatrol - 171625	Внедрение XML-кода

Symantec SIM

CVE ID	BugTraq ID	Date Discovered	Discovered By	
CVE-2006...		Mon Jul 11 11:12:10 MSD 20...	Qualys Guard Event Coll...	Oracle Enterprise Linux openssl Security Update (ELSA-2006:0661, ELSA-2
CVE-2006...		Mon Jul 11 11:12:10 MSD 20...	Qualys Guard Event Coll...	Oracle Enterprise Linux openssl Security Update (ELSA-2006:0661, ELSA-2
CVE-2006...		Mon Jul 11 11:12:10 MSD 20...	Qualys Guard Event Coll...	Oracle Enterprise Linux openssl Security Update (ELSA-2006:0661, ELSA-2
CVE-2006...		Mon Jul 11 11:12:10 MSD 20...	Qualys Guard Event Coll...	OpenOffice.org Multiple Vulnerabilities
CVE-2006...		Mon Jul 11 11:12:10 MSD 20...	Qualys Guard Event Coll...	Oracle Enterprise Linux openssl Security Update (ELSA-2006:0661, ELSA-2
CVE-2006...		Mon Ju		
CVE-2006...		Mon Ju		
CVE-2007...		Mon Ju		

General | Services | Access Rules | IPS Rule Groups | Routing Rules | Vulnerabilities | Attacks | Tickets

!	Exposure	Title	ID	CVE	Service Ports	Service Name
L	Unknown	Apache HTTP Server Vulnera...	SBV-15513	CVE-2006-5752	443/TCP	webserver (https)
M	Unknown	Apache HTTP Server 2.2-2.2...	SBV-17310	CVE-2007-6420	443/TCP	webserver (https)
M	Unknown	Apache 'mod_negotiation' Vu...	SBV-17856	CVE-2008-0456	443/TCP	webserver (https)
M	Unknown	Apache HTTP Server 2.2.0 - ...	SBV-17311	CVE-2007-6421	443/TCP	webserver (https)
H	Unknown	CUPS < 1.3.10 Web Interfac...	SBV-21818	CVE-2009-0164	443/TCP	webserver (https)
H	Unknown	Apache 2.2.11 and Prior mo...	SBV-22817	CVE-2009-1891	443/TCP	webserver (https)
M	Unknown	Apache HTTP Server < 2.2.6...	SBV-16069	CVE-2007-4465	443/TCP	webserver (https)
L	Unknown	Apache HTTP Server Cross S...	SBV-17314	CVE-2007-5000	443/TCP	webserver (https)
H	Unknown	Apache mod_proxy_http Re...	SBV-18597	CVE-2008-2364	443/TCP	webserver (https)
M	Unknown	Samba Oplock Break Notifica...	SBV-23613	CVE-2009-2906	139/TCP	netbios (netbios-ssn)

Skybox View

Cisco MARS

Vulnerability Information

Type
OpenSSL CBC Encryption Timing Attack
Apache 1.3.20 Large uri directory listing Vulnerability
Apache mod_ssl session caching buffer overflow
Apache 1.3.27 0x1A Character Logging DoS
Multiple Apache <=1.3.32 Web Server Local Buffer Overflow Vulnerabilities

Основная информация для экспорта

Операционные системы, открытые порты и службы

Symantec SIM

Port	Name	
53	domain	Domain Name Server (DNS)
88	kerberos	Kerberos v5
123	ntp	Network Time Protocol
137	netbios-ns	NETBIOS Name Service
139	netbios-ssn	NETBIOS Session Service
389	ldap	
445	microsoft-ds	
464	kpasswd	Kerberos passwd
636	lda	
135	ep	
593	htt	
1025	bla	

ArcSight ESM

Local Asset Categories
/All Asset Categories/Site Asset Categories/Application/Type/Database/SQLServer/Microsoft SQL Server 20
/All Asset Categories/Site Asset Categories/Application/JavaTM Platform 6, Standard Edition
/All Asset Categories/Site Asset Categories/Application/WinPcap
/All Asset Categories/Site Asset Categories/Application/Vendor/Microsoft/Microsoft Office Publisher MUI (Ru
/All Asset Categories/Site Asset Categories/Application/DAEMON Tools
/All Asset Categories/Site Asset Categories/Application/WinPcap 4.0.2
/All Asset Categories/Site Asset Categories/Application/WebFldrs XP
/All Asset Categories/Site Asset Categories/Application/Vendor/Microsoft/Microsoft Office Outlook MUI (Rus
/All Asset Categories/Site Asset Categories/Application/Vendor/Microsoft/Microsoft Office 2003 Web Compo
/All Asset Categories/Site Asset Categories/Application/Vendor/Microsoft/Microsoft Word
on/Type/Database/SQLServer/Microsoft SQL Server 20
rt/UDP/Port 500
on/Vendor/Microsoft/Microsoft Visual Studio
rt/TCP/Port 135
rt/UDP/Port 445

Skybox View

General | Services | Access Rules | IPS Rule Groups | Routing Rules | Vulnerabilities | Attacks | Tickets

Name	Type	Vendor	Ports
imap (imap)	Remote	Generic	143/TCP
imap (imaps)	Remote	Generic	993/TCP
ldap (ldap)			
microsoft-ds (microsoft-ds)			
mysql (mysql)			
ndl-aas (ndl-aas)			
netbios (netbios-ssn)			
pop3 (pop3)			
pop3 (pop3s)			

Cisco MARS

Service	Description	Source Ports	Destination Ports	Transport Protocol
VA Service (src port: ANY, dst port: 80, proto: TCP)		ANY	80	TCP
VA Service (src port: ANY, dst port: 443, proto: TCP)		ANY	443	TCP
VA Service (src port: ANY, dst port: 1521, proto: TCP)		ANY	1521	TCP
VA Service (src port: ANY, dst port: 135, proto: TCP)		ANY	135	TCP
VA Service (src port: ANY, dst port: 139, proto: TCP)		ANY	139	TCP
VA Service (src port: ANY, dst port: 1030, proto: TCP)		ANY	1030	TCP
VA Service (src port: ANY, dst port: 1032, proto: TCP)		ANY	1032	TCP
VA Service (src port: ANY, dst port: 1748, proto: TCP)		ANY	1748	TCP
VA Service (src port: ANY, dst port: 1754, proto: TCP)		ANY	1754	TCP

Интеграция MaxPatrol и Skybox View

- Экспорт осуществляется из локальной папки на сервере с установленным ПО Skybox View Collector
- Для экспорта используется XML-отчет MaxPatrol типа **SIEM integration file**
- Файл отчета должен быть назван **scan.xml**
- Экспорт осуществляется вручную или по заданному расписанию
- Обработанный файл остается на сервере

Интеграция MaxPatrol и Cisco MARS

- **Для экспорта данных обязательно создание веб-сервера**
- **На веб-сервере должен быть установлен PHP**
- **php-сценарии scan_report.php и scan_report_list.php находятся в каталоге установки MaxPatrol** (C:\Program Files\Positive Technologies\MaxPatrol\server\integration\mars)
- **Веб-сервер должен поддерживать одностороннюю аутентификацию по SSL** (необходимо создать сертификат для веб-сервера)
- **Для экспорта используется XML-отчет MaxPatrol типа SIEM integration file**
- **Экспорт осуществляется вручную или по заданному расписанию**
- **Обработанные файлы остаются на сервере**

Интеграция MaxPatrol и Symantec SIM

- Данные экспортируются из локальной папки на сервере с установленным ПО Symantec Event Agent и Qualys Guard collector
- После установки обязательно выполнить обновление Qualys Guard collector до версии 4.3
- Для экспорта используется XML-отчет MaxPatrol типа **SIEM integration file**
- Файл отчета должен иметь формат **<Sensor_name>_scan__*.xml**
- Экспорт осуществляется по заданному расписанию
- После экспорта файлы отчетов переименовываются или удаляются

Вопросы?

POSITIVE TECHNOLOGIES

MAXPATROL

Интеграция MaxPatrol и ArcSight ESM

- **Данные экспортируются из сетевой папки** (необходим доступ к этой папке для коннектора ArcSight)
- **Тип используемого коннектора – ArcSight FlexConnector Scanner XML Reports**
- **Для экспорта используется XML-отчет MaxPatrol типа XML file**
- **Конфигурационные файлы коннектора размещаются в директории установки MaxPatrol** (C:\Program Files\Positive Technologies\MaxPatrol\server\integration\arcsight)
- **Экспорт осуществляется вручную или автоматически в режиме реального времени**
- **После экспорта файлы отчетов переименовываются или удаляются**

Что экспортируется в ArcSight ESM?

PenTest

- Данные о сканировании
- Данные об узлах (IP, hostname, FQDN)
- Открытые порты, протоколы, службы
- Обнаруженные уязвимости (с указанием уязвимого приложения, уровня опасности уязвимости, рекомендаций по исправлению, оценок по CVSS и идентификаторов уязвимости в различных системах трекинга)
- Вероятные версии ОС

Audit

- Данные о сканировании
- Данные об узлах (IP, hostname, FQDN, MAC)
- Открытые порты, протоколы, службы
- Обнаруженные уязвимости
- Версии ОС
- Данные об аппаратном обеспечении
- Данные о программном обеспечении

Compliance

- Данные о сканировании
- Данные об узлах (IP, hostname, FQDN)
- Наименование стандарта
- Идентификатор требования в системе MaxPatrol и его статус (выполнено/не выполнено/ не применимо/не известно/не проверялось)
- Содержание требования
- Рекомендации по достижению соответствия