MaxPatrol 8

POSITIVE TECHNOLOGIES

ptsecurity.ru

Positive Technologies:

в цифрах и фактах

О нас

POSITIVE TECHNOLOGIES

Каждый год

200+
аудитов безопасности корпоративных систем

200+
обнаруженных уязвимостей нулевого дня

Главные продукты

- MaxPatrol
- MaxPatrol SIEM
- PT ISIM
- PT Application Firewall

Визионер 2016
WAF Magic Quadrant
Gartner®

15 **лет исследований и экспертизы**

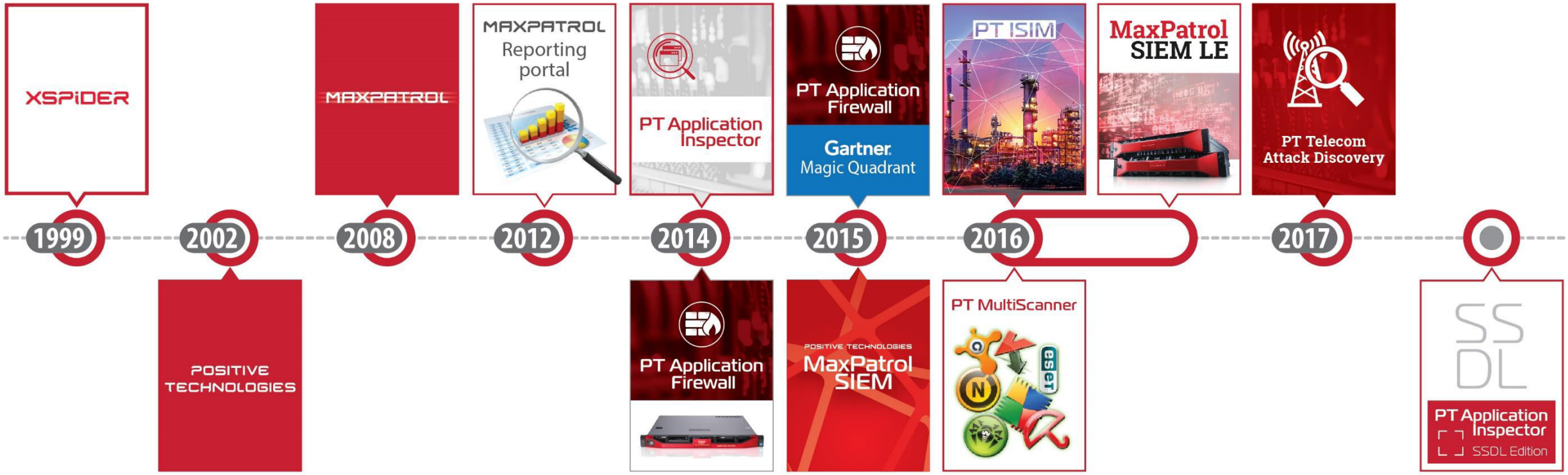
150+ уязвимостей нулевого дня в системах SCADA

30+ обнаруженных уязвимостей нулевого дня в Mobile Telco

500+ исследований безопасности мобильных и веб-приложений

Наша история

POSITIVE TECHNOLOGIES



Наши заказчики

POSITIVE TECHNOLOGIES

Финансы, страхование

РОСБАНК

СБЕРБАНК

Райффайзен БАНК

Альфа-Банк

ВТБ24

ГАЗПРОМБАНК

INTESA SANPAOLO

ИНГОССТРАХ Ingosstrakh

UniCredit

Телекоммуникации

Ростелеком

МегаФон

МТС

Tre.it

Билайн

SK telecom

Промышленность, энергетика

Газпром

ЛУКОЙЛ НЕФТЯНАЯ КОМПАНИЯ

ТМК

РусГидро

РОСАТОМ

НОРНИКЕЛЬ

РОССЕТИ

НИЖНЕКАМСКНЕФТЕХИМ

IRKUT ИРКУТ

В СОСТАВЕ ОАК КОРПОРАЦИЯ ИРКУТ

Госсектор

ФНС

МВД

Минобороны

ФСТЭК

ПФР

ГОЗНАК

ФТС

MaxPatrol 8.

Контроль защищенности и соответствия стандартам

Наша статистика

POSITIVE TECHNOLOGIES

Каждую **вторую** систему может взломать неквалифицированный хакер

Защита периметра не останавливает проникновение

Атак могли быть предотвращены стандартными решениями

Инцидентов стали успешными из-за серьезных ошибок в конфигурации

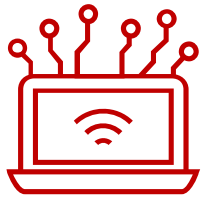
Атак не требовали высокой квалификации нарушителей

Источник: Positive Research 2017

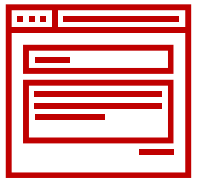
Почему инфраструктура уязвима

POSITIVE TECHNOLOGIES

Слабые пароли



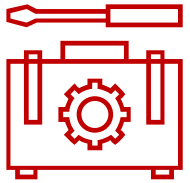
Небезопасные беспроводные сети



Уязвимости веб-приложений

Программное обеспечение

Социальная инженерия



Ошибки в настройках:

- сетевого оборудования
- систем защиты периметра
- веб-приложений
- баз данных

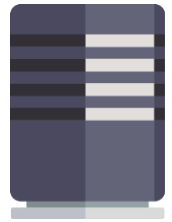
Процесс управления уязвимостями

POSITIVE TECHNOLOGIES

– Требует наличия узкопрофильных специалистов

– Длительное время обслуживания каждого компонента ИС

– Высокая роль человеческого фактора



\+ Использует единые подходы для анализа всех компонентов ИС

\+ Производится на регулярной основе автоматически

\+ Формирует унифицированную отчетность

Maxpatrol 8 – решение

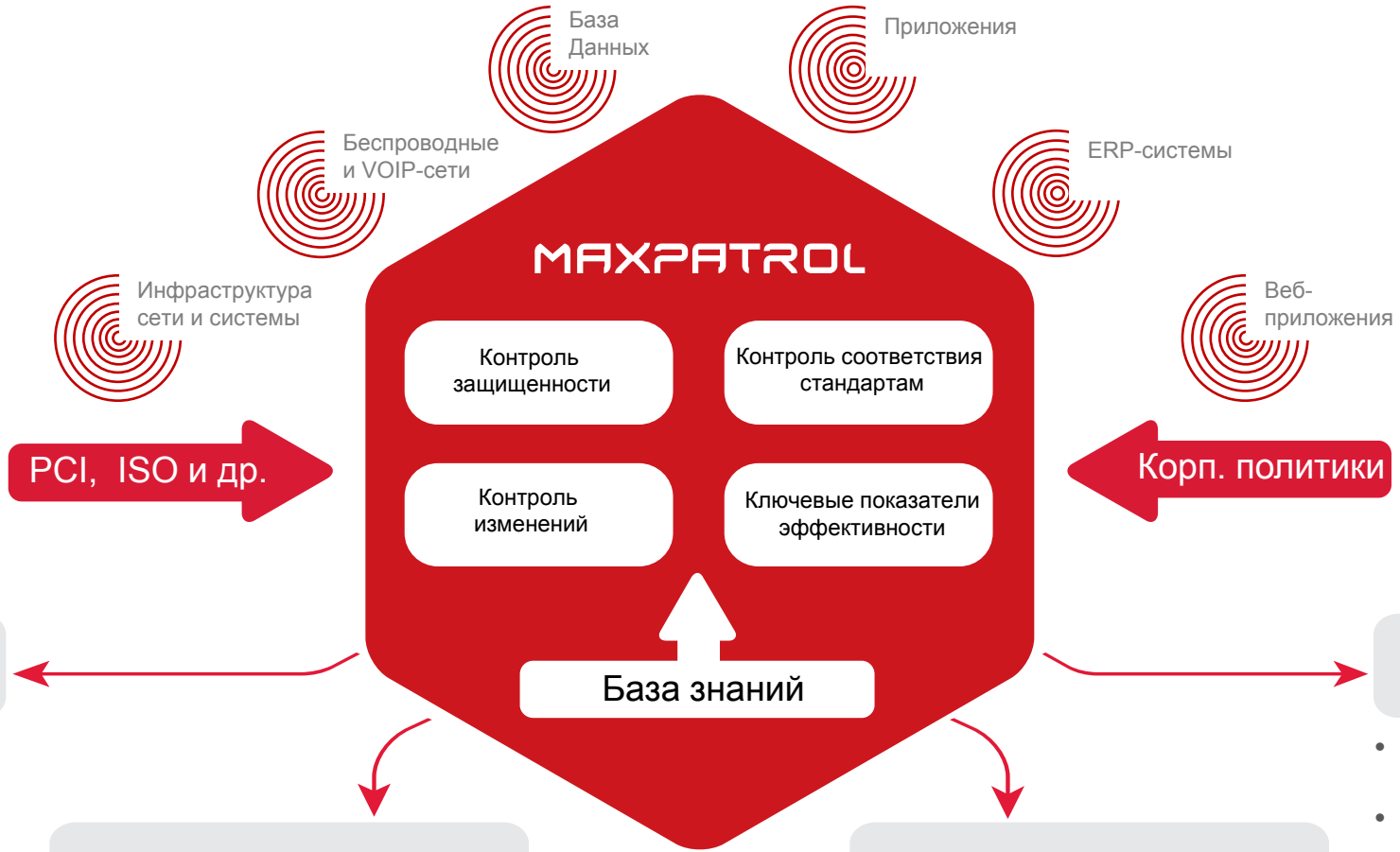
POSITIVE TECHNOLOGIES

1. Инвентаризация
и контроль конфигураций
2. Комплексная
оценка защищенности
3. Автоматизация
контроля соответствия требованиям
4. Технические
и высокоуровневые отчеты
5. Ежедневно обновляемая
база знаний

продукт года в категории
Vulnerability Management по версии британской премии **Cyber Security Awards 2016**

Функции системы

POSITIVE TECHNOLOGIES



Руководители

- Снижение человеческого фактора за счет автоматизации
- KPI отчетность по бизнес-подразделениям
- Соответствие стандартам организации
- Данные о текущем уровне защищенности

Специалисты по ИБ

- Выявление уязвимостей
- Управление соответствием стандартам
- Контроль соответствия политикам
- Контроль устранения уязвимостей

Специалисты по ИТ

- Простота внедрения
- Инвентаризация ресурсов ИТ
- Рекомендации по устранению
- Отчетность по обновлениям

Аудиторы

- Комплексный инструмент для оценки защищенности
- Поддержка основных международных стандартов
- Настраиваемая система отчетности

MaxPatrol 8.

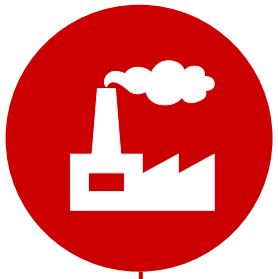
Особые сценарии использования

Дополнительные сценарии

POSITIVE TECHNOLOGIES

ERP

- SAP NetWeaver™
- SAP R/3
- SAP R/3 ENTERPRISE



АСУ ТП

- SIEMENS
- invensys
- Rockwell Automation
- Schneider Electric

ТЕЛЕКОМ

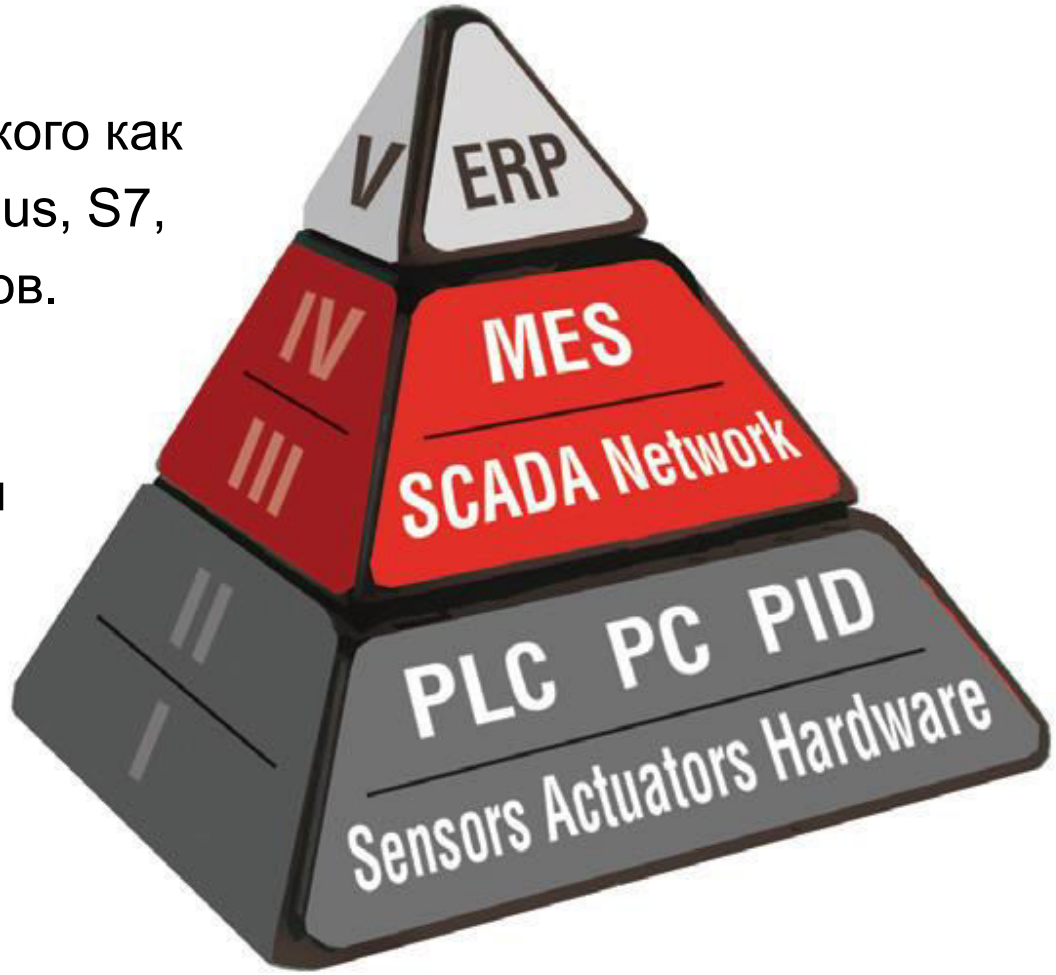
- HUAWEI
- ERICSSON

MaxPatrol 8 для SCADA

POSITIVE TECHNOLOGIES

MaxPatrol имеет встроенные проверки для специализированного сетевого оборудования, такого как Cisco Connected Grid, реализует поддержку Modbus, S7, DNP3, IEC104 и других промышленных протоколов.

База знаний содержит более **30 000** проверок на уязвимости и требования по безопасности для *HMI/SCADA, PLC, RTU* ведущих производителей: **Siemens, Schneider Electric, Rockwell Automation, ABB.**



MaxPatrol 8 для Телеком

POSITIVE TECHNOLOGIES

1 УСТРАНЕНИЕ ПЕТЕЛЬ КОММУТАЦИИ HUAWEI

		Ст.	ID	Полное описание
Соответствует	10.176.71.196	SP	436196	Включить Loopback-detection на интерфейсах S33/S53-NNI, S33/S53-UNI и S33/S53-ext-NNI
Соответствует	10.176.71.198			
Соответствует	10.176.71.199			
Соответствует	10.176.71.200			
Соответствует	10.176.71.201			
Соответствует	10.176.71.202			
Соответствует	10.176.71.203			
Не соответствует	10.176.71.204			
Не соответствует	10.176.71.205			
Не соответствует	10.176.71.206			
Не соответствует	10.176.71.207			
Не соответствует	10.176.71.208			
Не соответствует	10.176.71.209			
Не соответствует	10.176.71.210			
Не соответствует	10.176.71.223			
Соответствует	10.176.71.225			
Соответствует	10.176.71.226			
Соответствует	10.176.71.227			
Соответствует	10.176.71.228			
Соответствует	10.176.71.229			
Соответствует	10.176.71.230			
Соответствует	10.176.71.231			
Соответствует	10.176.71.234			

Детальная информация по требованиям

Не соответствует — Технические требования, которые переопределены пользователем

Включить Loopback-detection на интерфейсах S33/S53-NNI, S33/S53-UNI и S33/S53-ext-NNI

ID: 436196

--

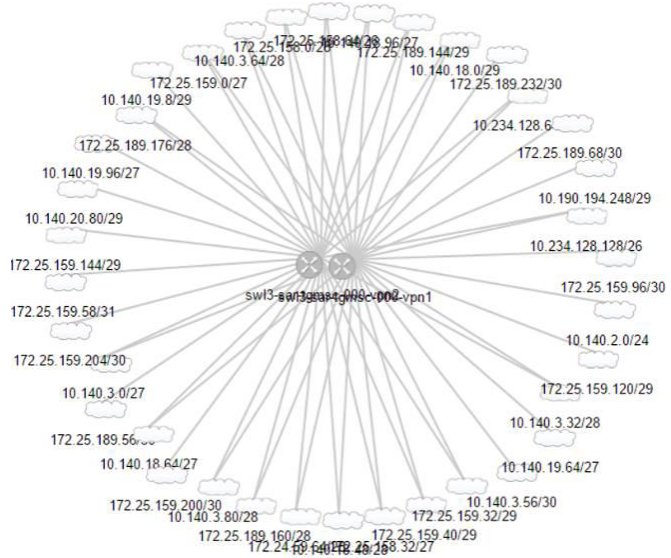
Название блока	Значение	Несоответствие	Статус
interface Aux0/0/1	link-protocol ppp undo shutdown		Входит в список исключений
interface GigabitEthernet0/0/0	speed auto duplex auto undo shutdown		Входит в список исключений
interface GigabitEthernet1/0/0	carrier up-hold-time 10000 description BSC_OAM_1c7819348_REZERV_TT7418948 undo shutdown set flow-stat interval 10 mtu 9600 l2 binding vsi BSC_OAM undo dcn trust upstream default trust 8021p	loopback-detect enable	Не соответствует требованию
interface GigabitEthernet1/0/1	carrier up-hold-time 10000 description BSC_OAM_Beloreck_1C7910932 undo shutdown set flow-stat interval 10 mtu 9600 l2 binding vsi BSC_OAM_Beloreck_1C7923386 undo dcn loopback-detect enable trust upstream not_6_7 trust 8021p undo lldp enable		Соответствует требованию

GGSN

RNC

Node B

2 ПОСТРОЕНИЕ ТОПОЛОГИИ MEN-СЕТЕЙ



3 КОНТРОЛЬ СООТВЕТСТВИЯ LOW LEVEL DESIGN

4 АУДИТ MEN-СЕТЕЙ

MaxPatrol 8 для SAP

POSITIVE TECHNOLOGIES

СООТВЕТСВИЕ ТРЕБОВАНИЯМ ТЕХНИЧЕСКИХ СТАНДАРТОВ

- для прикладного
- для системного
- для сетевого
- для пользовательского уровней

ИНВЕНТАРИЗАЦИЯ КОМПОНЕТОВ СИСТЕМЫ

- серверы приложений SAP
- серверы СУБД
- рабочие станции
- сетевое оборудование
- средства защиты

ВЫЯВЛЕНИЕ И УСТРАНЕНИЕ ТЕХНИЧЕСКИХ УЯЗВИМОСТЕЙ

- SAP R/3 и SAP R/3 Enterprise;
- SAP NetWeaver AS ABAP;
- SAP NetWeaver AS JAVA;
- Бизнес модулей SAP
- SAPRouter

АНАЛИЗ КОНФИГУРАЦИЙ СИСТЕМЫ И ЕЕ КОМПОНЕТОВ

- системные параметры
- бизнес модули (ERP, HR, MM)
- сервисы SAP системы
- настройки шифрования
- неиспользуемые RFC-соединения
- статус учетных записей и критичные полномочия

SAP® Certified
Integration with SAP NetWeaver®

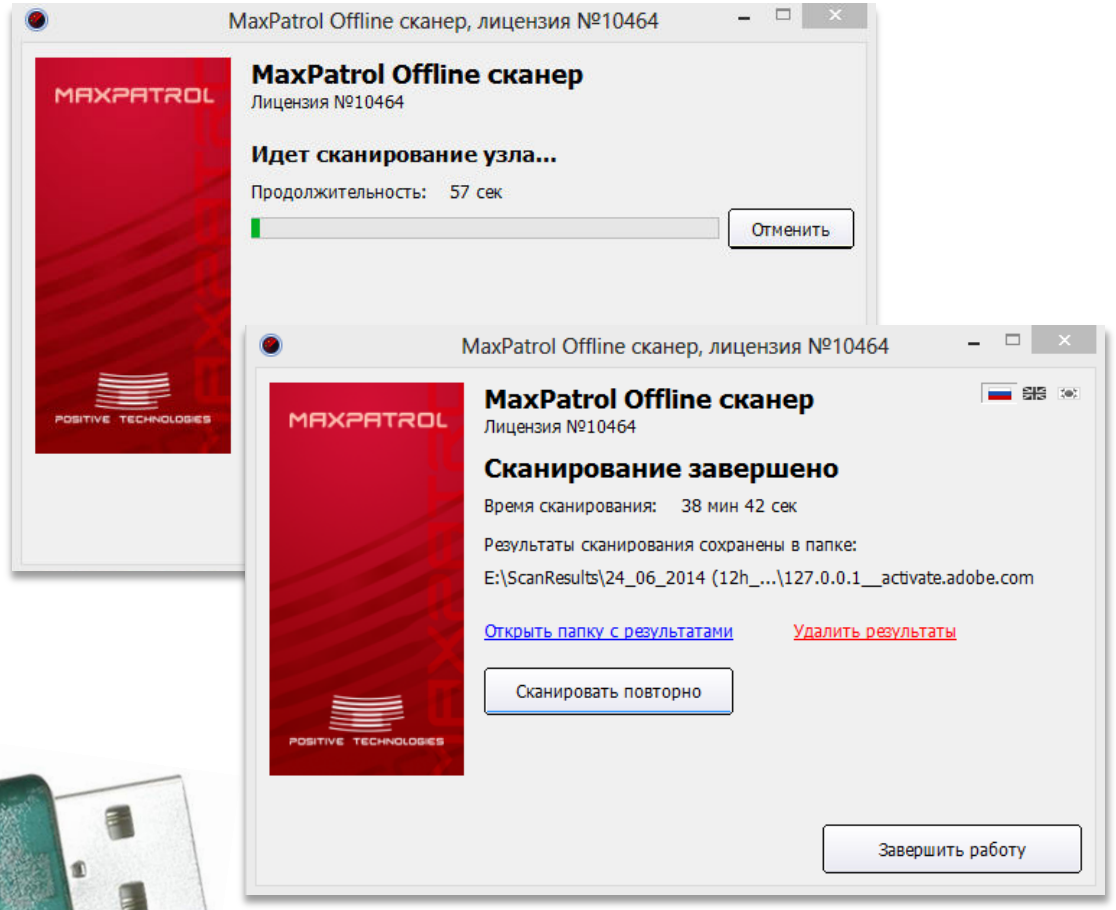
Offline-сканнер

POSITIVE TECHNOLOGIES

Компонент **offline-сканер** предназначен для сканирования узлов, изолированных от локальной сети.

Он позволяет произвести полноценное сканирование Windows-систем в режимах **pentest, audit, compliance, forensic.**

Сканирующий **offline-модуль** размещается на специализированном USB-носителе.



Поддерживаемые системы

POSITIVE TECHNOLOGIES

1000+ систем,
с которыми умеет работать MaxPatrol 8, среди них:

Операционные системы




Базы данных




Сетевое оборудование




Инфраструктурные приложения




Решения виртуализации




Настольные приложения





Средства безопасности








Схема работы

POSITIVE TECHNOLOGIES

РЕСУРСЫ

- Настольные Приложения
- Операционные системы
- Сетевое оборудование
- СУБД
- SAP
- ВЕБ
- Виртуальные среды
- VPN
- АСУ ТП
- Антивирусы

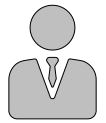
PCI DSS, ISO 27001, Персональные данные

COMPLIANCE	• Контроль соответствия стандартам
AUDIT	• Системные проверки • Анализ конфигураций • Анализ ПО • Инвентаризация
PENTEST	• Поиск уязвимостей • Сетевое сканирование • Аудит веб-приложений • Сканирование СУБД

База знаний уязвимостей и ПО

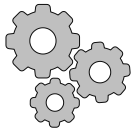
Корпоративные стандарты

ОТЧЕТНОСТЬ



УПРАВЛЕНЧЕСКАЯ

АНАЛИТИЧЕСКАЯ



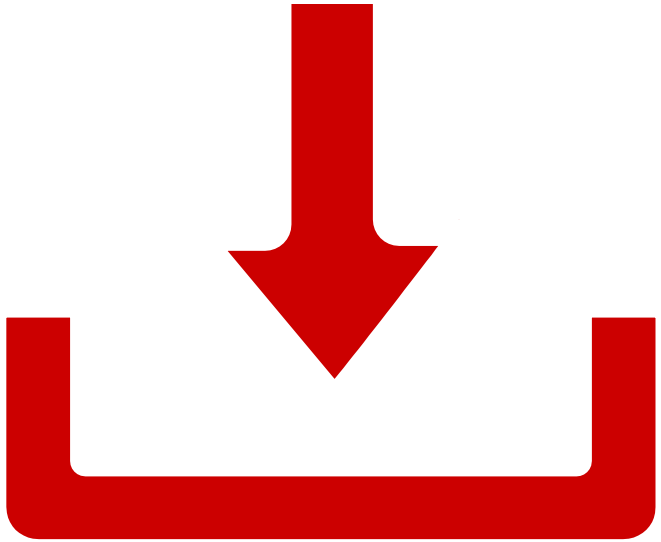
ТЕХНИЧЕСКАЯ

- Соответствие стандартам
- Инвентаризация активов
- Динамика изменений
- Данные по уязвимостям

Режим Pentest

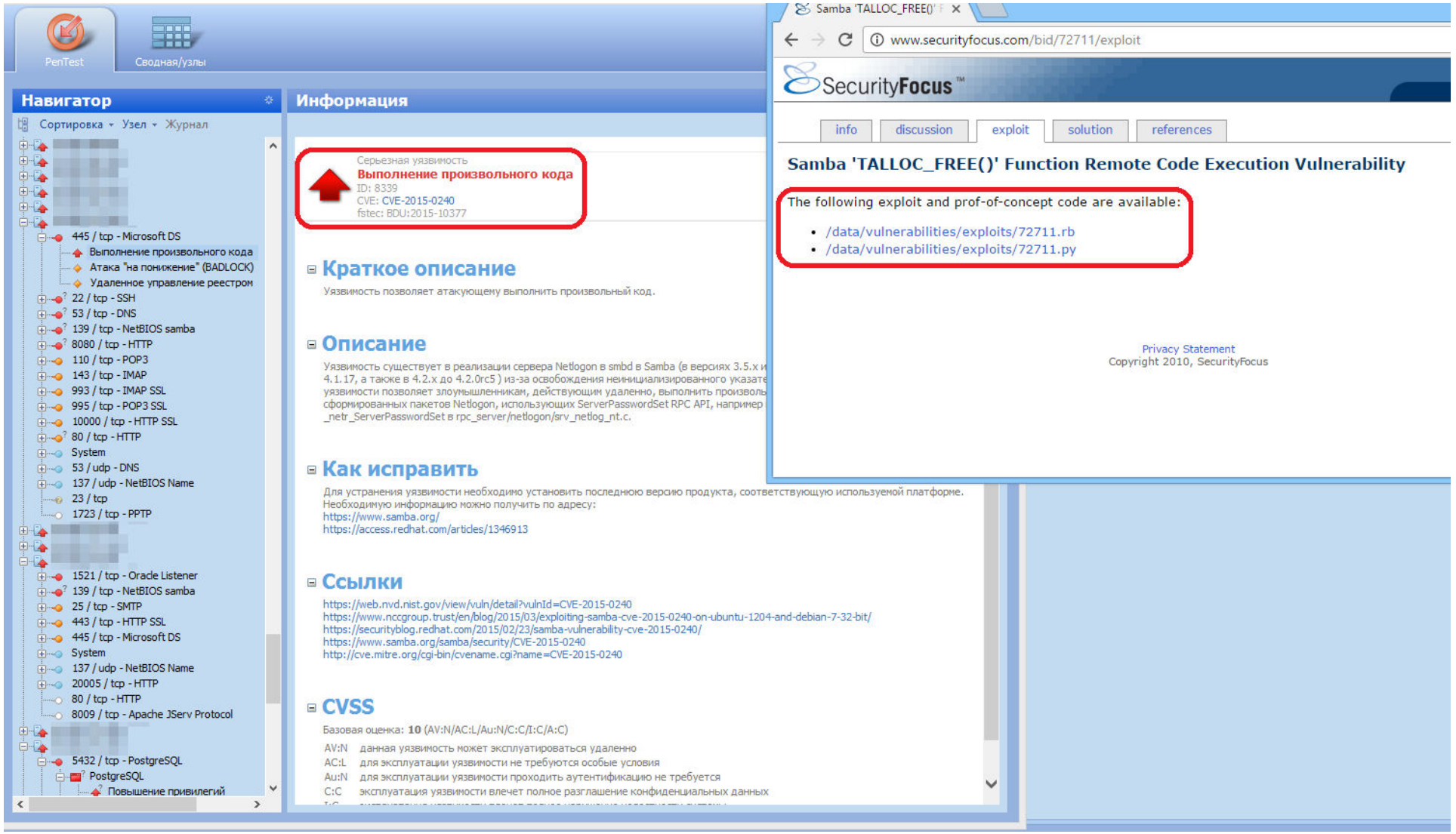
POSITIVE TECHNOLOGIES

- Анализ в режиме «черного ящика»
- Определяет уязвимости:
  - путем анализа сообщений (баннеров)
  - используя логику работы эксплойтов
  - эвристическими методами
- Анализирует веб-приложения
- Перебирает пароли
- Диагностирует сетевые службы



Режим Pentest (скриншот)

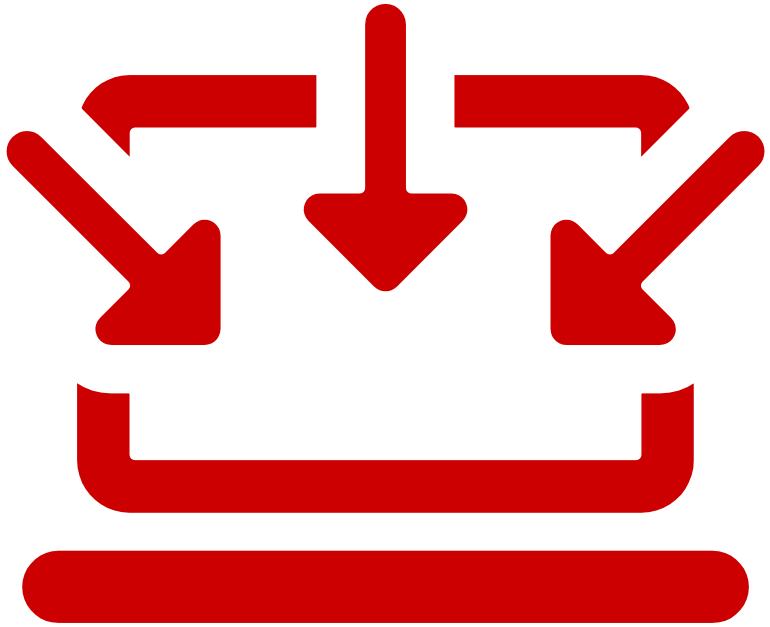
POSITIVE TECHNOLOGIES



Режим Audit

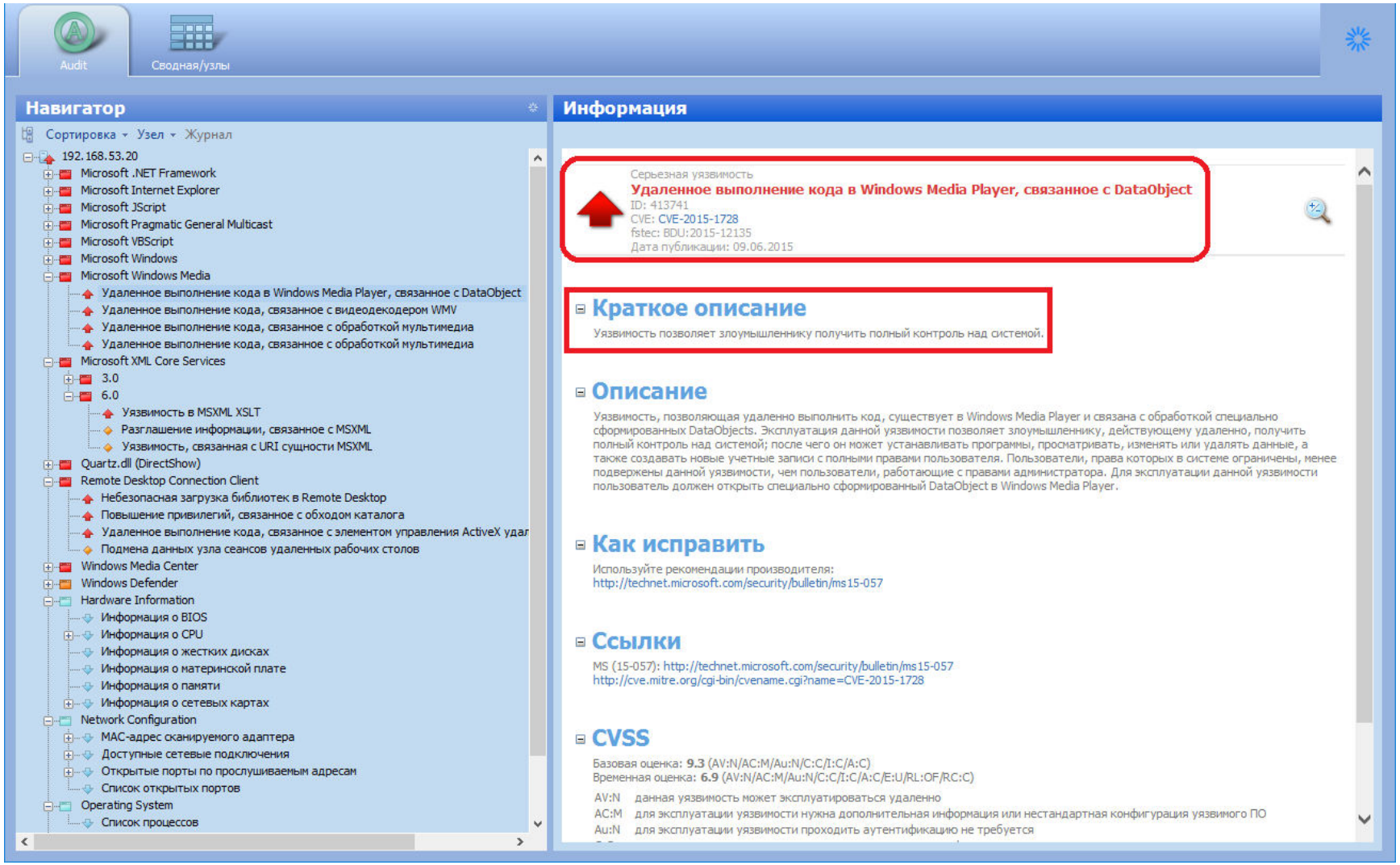
POSITIVE TECHNOLOGIES

- Не требует установки агента
- Использует стандартные протоколы удаленного доступа
  - Инвентаризация аппаратного и программного обеспечения
  - Проверки наличия обновлений безопасности
  - Выявление наличия уязвимостей и ошибок конфигураций
  - Анализ конфигурации
  - Контроль учетных записей
  - Контроль изменений



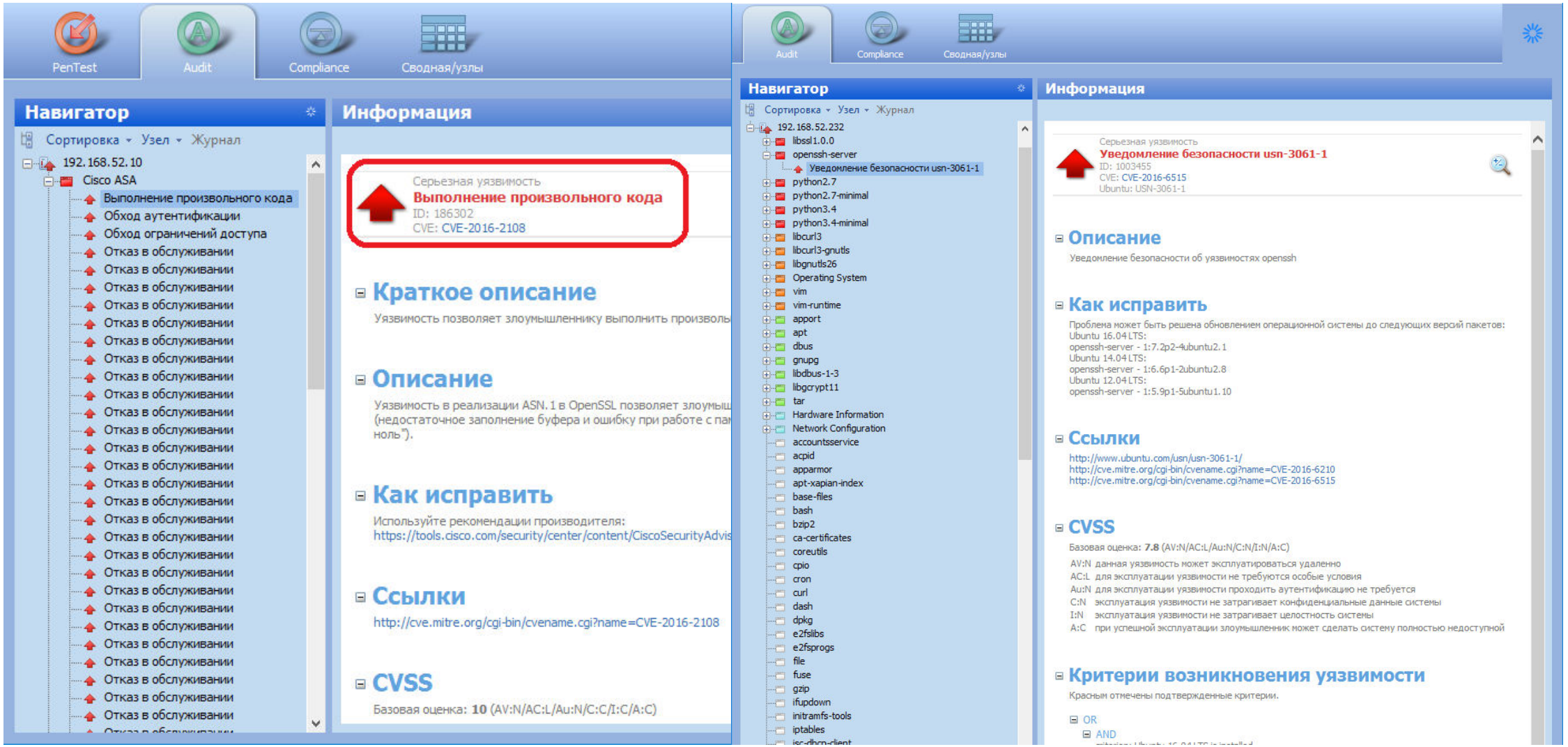
Режим Audit (скриншот)

POSITIVE TECHNOLOGIES



Режим Audit (скриншот)

POSITIVE TECHNOLOGIES



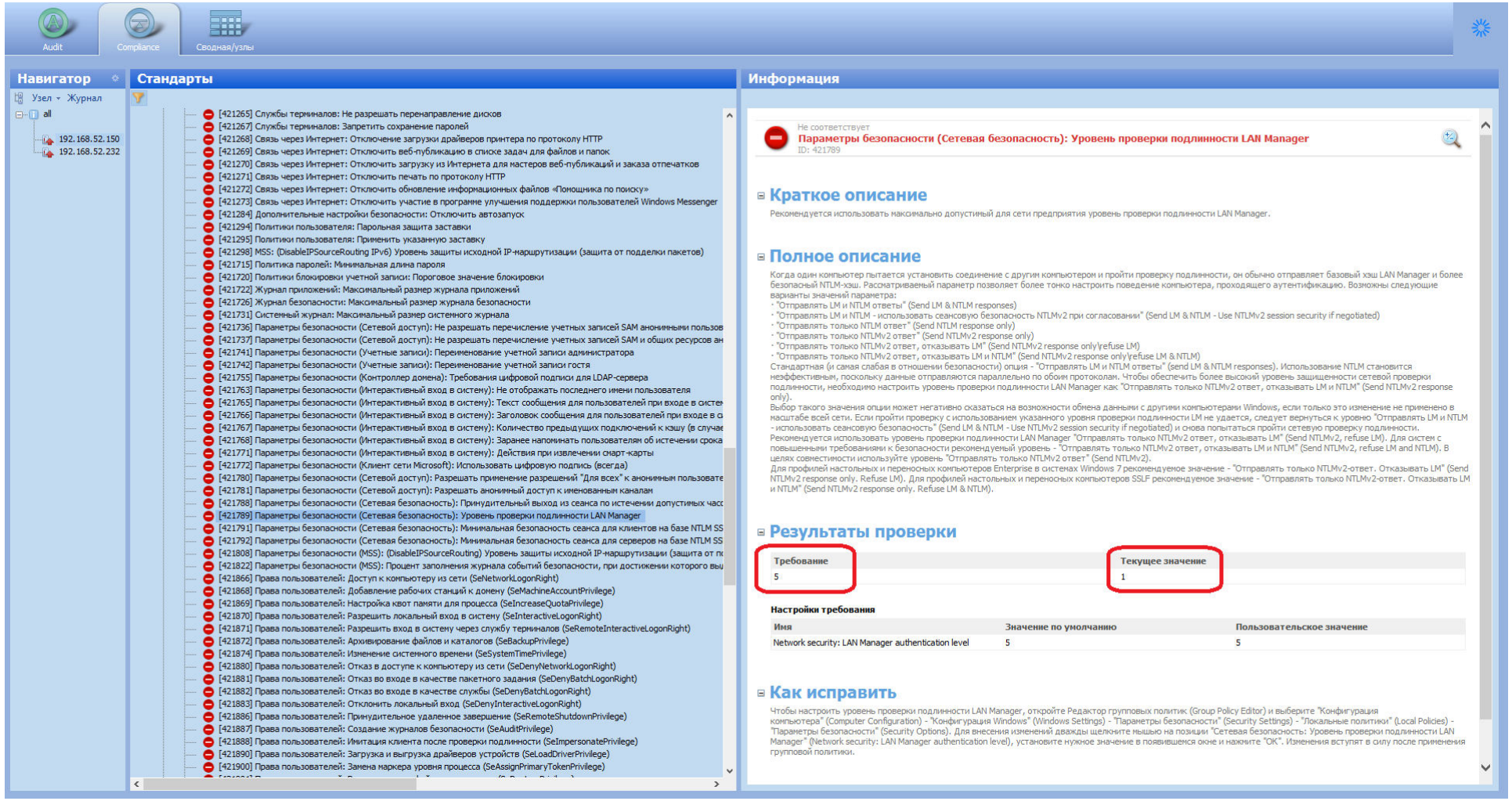
Режим Compliance

POSITIVE TECHNOLOGIES

- Более **150** встроенных стандартов
- Автоматическое определение соответствия применимым стандартам
- Поддержка высокоуровневых стандартов и требований регуляторов
  - 152-ФЗ «О персональных данных»
  - СТО БР ИББС
  - PCI DSS
  - ISO 27001/27002
  - Приказы ФСТЭК 17, 21, 31
- Контроль выполнения собственных корпоративных правил безопасности

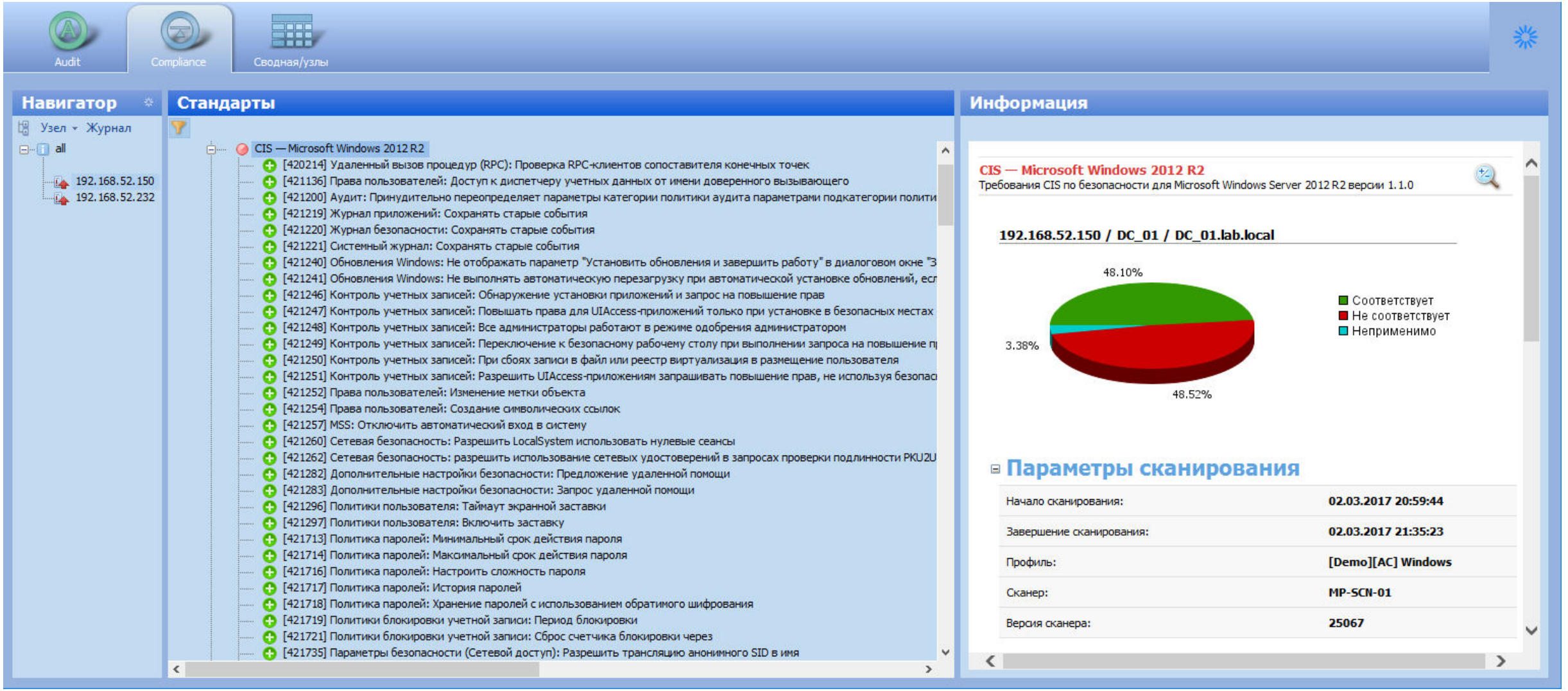
Режим Compliance (скриншот)

POSITIVE TECHNOLOGIES



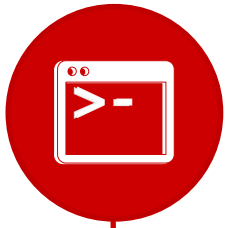
Режим Compliance (скриншот)

POSITIVE TECHNOLOGIES

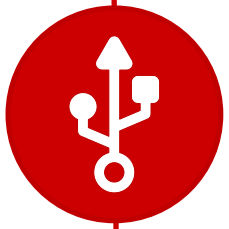


Дополнительные возможности

POSITIVE TECHNOLOGIES



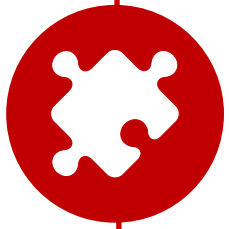
Контроль установленного ПО



Контроль подключенных USB-устройств

Контроль сетевых настроек

Контроль парольной политики



Контроль целостности

Контроль средств защиты

Контроль изменений

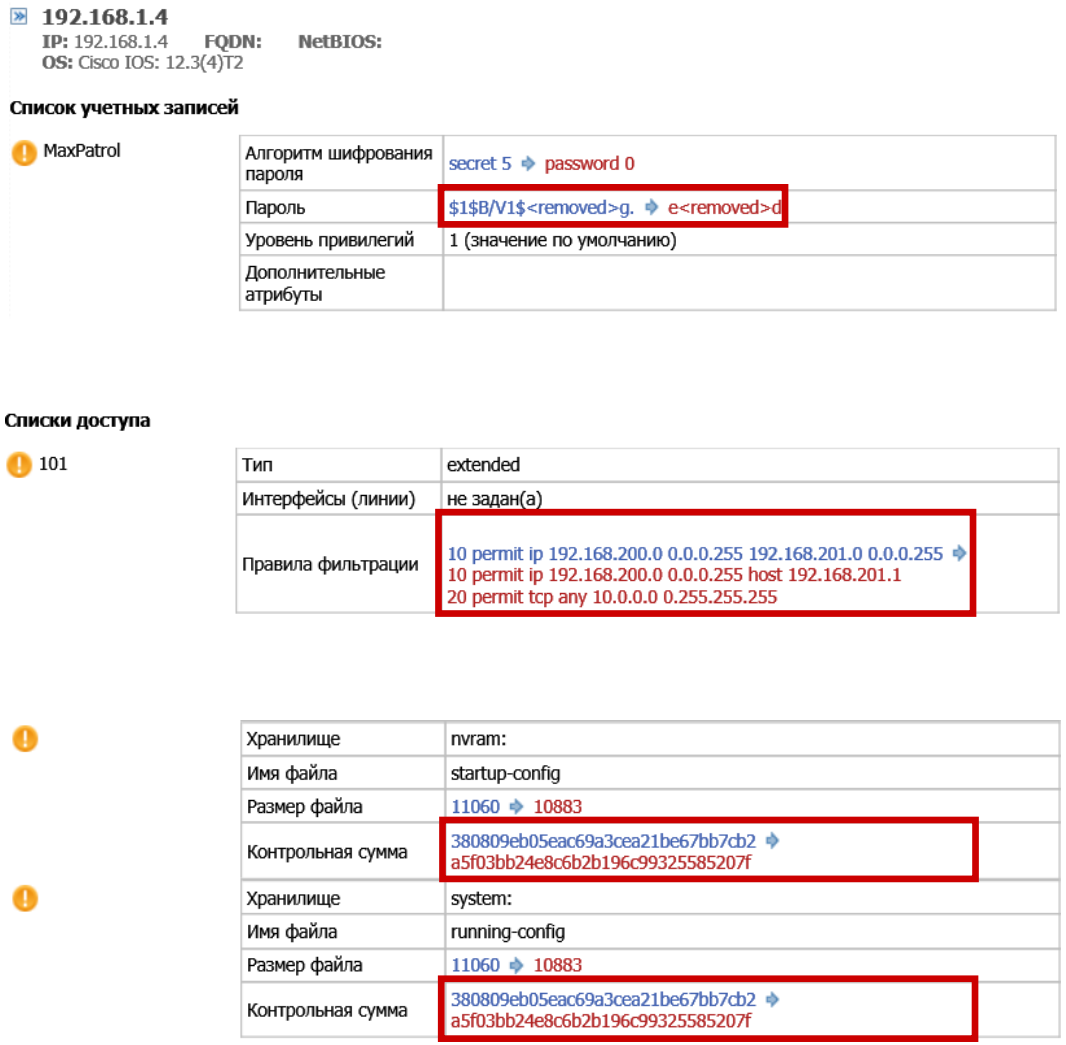
POSITIVE TECHNOLOGIES

Дифференциальные отчеты – уведомление об изменениях в инфраструктуре:

1. **Смена пароля**

2. **Модификация списков контроля доступа**

3. **Изменение контрольных сумм файлов**



192.168.1.4
IP: 192.168.1.4 **FQDN:** **NetBIOS:**
OS: Cisco IOS: 12.3(4)T2

Список учетных записей

MaxPatrol

Алгоритм шифрования пароля	secret 5 ➧ password 0
Пароль	1B/V1$<removed>g. ➧ e<removed>d
Уровень привилегий	1 (значение по умолчанию)
Дополнительные атрибуты	

Списки доступа

101

Тип	extended
Интерфейсы (линии)	не задан(а)
Правила фильтрации	10 permit ip 192.168.200.0 0.0.0.255 192.168.201.0 0.0.0.255 ➧ 10 permit ip 192.168.200.0 0.0.0.255 host 192.168.201.1 20 permit tcp any 10.0.0.0 0.255.255.255

Хранилище	nvram:
Имя файла	startup-config
Размер файла	11060 ➧ 10883
Контрольная сумма	380809eb05eac69a3cea21be67bb7cb2 ➧ a5f03bb24e8c6b2b196c99325585207f
Хранилище	system:
Имя файла	running-config
Размер файла	11060 ➧ 10883
Контрольная сумма	380809eb05eac69a3cea21be67bb7cb2 ➧ a5f03bb24e8c6b2b196c99325585207f

Интеграционные возможности

POSITIVE TECHNOLOGIES

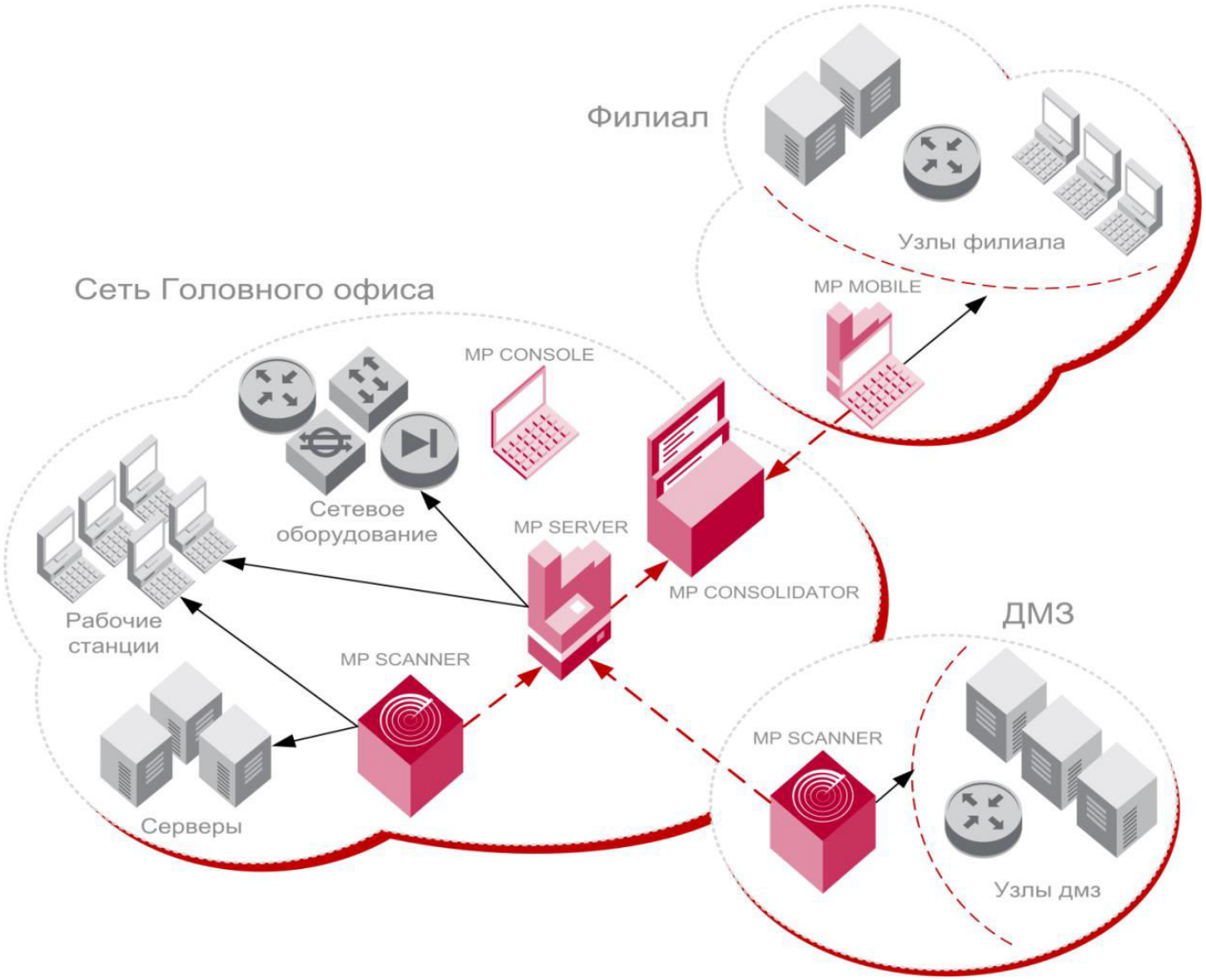
- Управление активами
- Help Desk системы
- Управление рисками
- Управление установкой исправлений
- SIM/SIEM
- IDM

Архитектура Maxpatrol 8

POSITIVE TECHNOLOGIES

КОМПОНЕНТЫ

- **MP Server**
- **MP Scanner**
- **MP Consolidator**
- **MP Console**
- **MP Mobile Server**
- **MP Local Update Server**



Встроенные отчеты

POSITIVE TECHNOLOGIES

MAXPATROL 06.03.2017 17:53:13

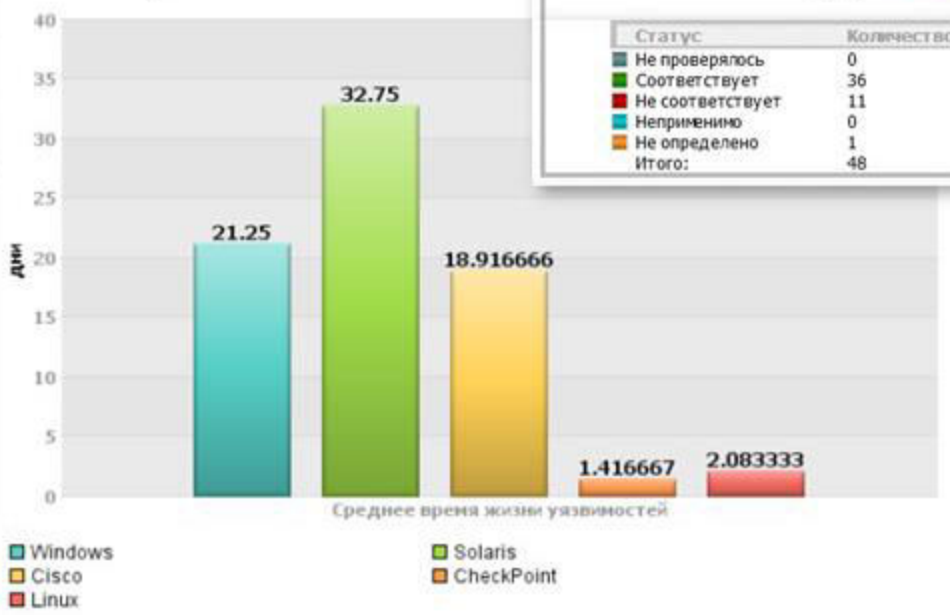
Рейтинг уязвимостей

Vulnerability rating

Vulnerability	CVE	Quantity
usn-3134-1: python2.7, python3.2, python3.4, python3.5 vulnerabilities	CVE-2016-5699	4
usn-3134-1: python2.7, python3.2, python3.4, python3.5 vulnerabilities	CVE-2016-5636	4
usn-3134-1: python2.7, python3.2, python3.4, python3.5 vulnerabilities	CVE-2016-0772	
Memory Leak	CVE-2016-6304	2
Integer Overflow	CVE-2016-6303	2
Denial of Service	CVE-2016-2182	2
.NET XML Validation Security Feature Bypass	CVE-2016-0132	2
Denial of Service	CVE-2017-0016	1

MAXPATROL

Среднее время жизни уязвимостей

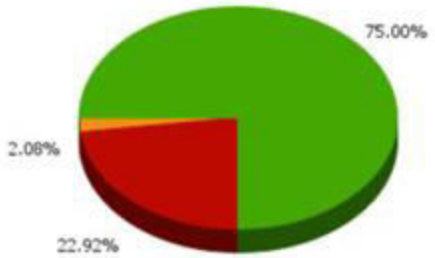


MAXPATROL 06.03.2017 17:53:13

Symantec

Compliance: PT - Symantec Anti-Virus

Интегральные данные по требованиям всех узлов и задач



Статус	Количество проверок	Доля проверок
Не проверялось	0	0%
Соответствует	36	75%
Не соответствует	11	22.91%
Неприменимо	0	0%
Не определено	1	2.08%
Итого:	48	100%

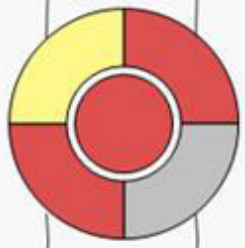
Аналитический онлайн-портал: общая картина

POSITIVE TECHNOLOGIES

Показатели информационной безопасности инфраструктуры за Q3

Контроль защищенности

Обнаружено High уязвимостей		29,3%
Обнаружено Medium уязвимостей		41,7%
Количество уязвимостей больше, чем в	Q2, на	-
Количество узлов с High уязвимостями		49,3%
Количество узлов с Medium уязвимостями		26,6%
Количество уязвимых узлов выросло с	Q2 на	-



Контроль эффективности ИБ

Устранено уязвимостей		-
План сканирования узлов выполнен на		29,3%
Количество просканированных узлов выросло с	Q2 на	-38,4%
Заданная регулярность сканирования узлов соблюдена на		50,4%
План ввода в эксплуатацию компонентов МР выполнен на		23,4%
Работоспособность компонентов МР за период		---

Управление активами

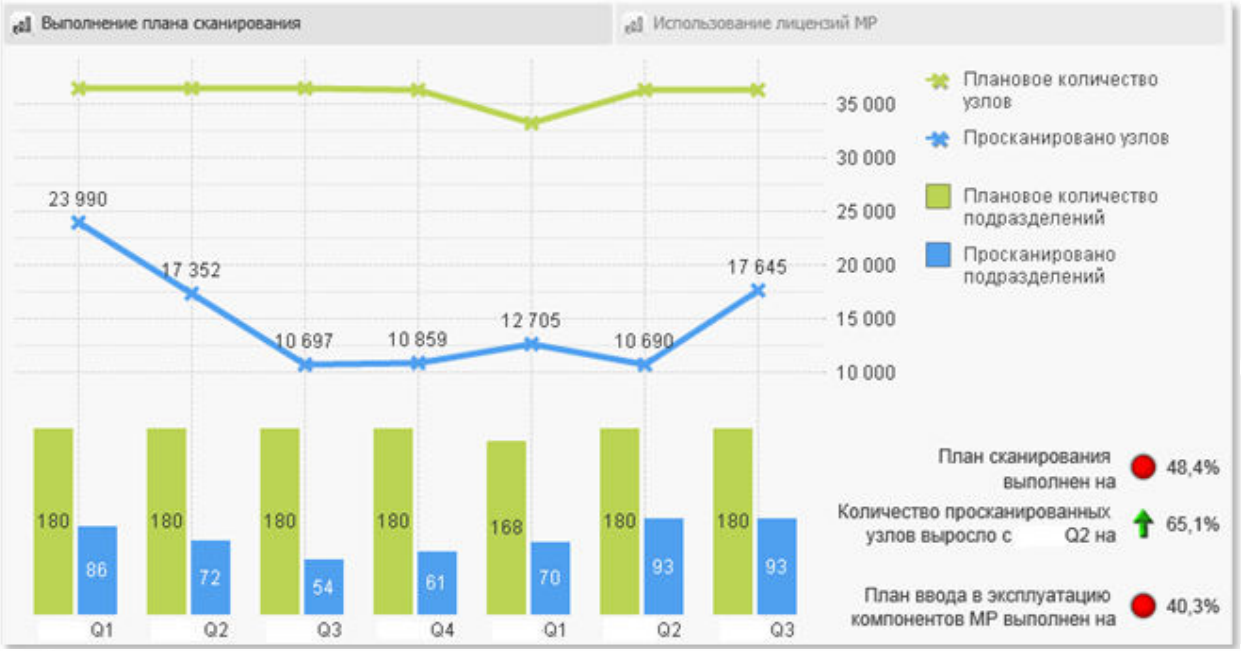
Количество узлов с запрещенным ПО	3,7%
Количество узлов с обязательным ПО	16,7%
Соблюдение лицензионной политики	---
Использование запрещенного оборудования	---

Соответствие стандартам

Подразделение	Статус
Управление по Архангельской области	
Управление по Архангельской области	
Подразделение № 31	
Подразделение № 1	
Подразделение № 7	
Управление по Астраханской области	
Управление по Брянской области	
Управление по г.Москве	
Управление по г.Санкт-Петербургу	

Аналитический онлайн-портал: детализация

POSITIVE TECHNOLOGIES



Самые уязвимые узлы

Идентификатор узла	High	Medium	Low
10.1.34.112	118	1	1
10.1.120.22	19	9	4
10.1.124.45	18	2	4
10.1.230.46	17	29	7
10.1.96.29	17	4	5
10.1.230.53	16	8	5
10.1.230.52	16	5	6
10.1.64.45	15	13	9
10.1.203.211	15	3	4
	8 660	**28 959**	**18 296**

Самые распространенные уязвимости

Ур...	Уязвимость	Узлов	Оценка CVSS
High	Уязвимость RPC делает возможной атаку т	1 533	0
High	Учетная запись пользователя	1 297	0
High	Удаленное управление реестром	606	0
High	Найден пароль	489	0
High	Удаленное выполнение кода при переполн	340	6,1
High	Отказ в обслуживании при проверке SMB	340	4,8

Обнаруженные уязвимости

ID		Уязвимость	Оценка CVSS		Подраз	Узлы		Распространение	Идентификатор уязвимости
412022	High	Уязвимость RPC делает возможной атаку типа "отказ в обслуживании"		(+2) ↑	72	1533	(+561)		CVE-2007-2228
1205	High	Учетная запись пользователя		(+8) ↑	59	1297	(+1 166)		-
6015	High	Найдены учётные записи	8,7	(-1) ↓	49	293	(+120)		-
1066	High	Удаленное управление реестром		(+1) ↑	66	606	(+332)		-
412205	High	Удаленное выполнение кода при переполнении SMB -буфера	6,1		48	340	(+59)		CVE-2008-4834

Обоснование внедрения

POSITIVE TECHNOLOGIES

Применение MaxPatrol 8 позволяет выполнить ряд требований регуляторов:

- **Приказ ФСТЭК №17 от 11.02.2013г.**
  «Об утверждении требований о защите информации, не составляющей государственную тайну»
- **Приказ ФСТЭК №21 от 18.02.2013г.**
  «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
- **Приказ ФСТЭК №31 от 14.03.2014г.**
  «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а так же объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

Обоснование внедрения

POSITIVE TECHNOLOGIES

Применение MaxPatrol 8 позволяет выполнить ряд требований регуляторов:

- **РС БР ИББС – 2.6-2014.**
  «Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем»
- **Payment Card Industry Data Security Standard (PCI DSS v3.2).**
  «Требования и процедуры аудита безопасности»
- **ISO/IEC 27001/27002.**
  «Системы менеджмента информационной безопасности», «Свод рекомендуемых правил для управления информационной безопасностью»

Преимущества использования Maxpatrol 8

POSITIVE TECHNOLOGIES

- **Автоматизация поиска и устранения уязвимостей**
- **Стандарты ИБ для ИС и прикладного ПО**
- **Оптимизация использования средств защиты**
- **Регулярная оценка эффективности работы отделов ИТ и ИБ**
- **Повышения уровня защищенности ИС**
- **Сокращение финансовых затрат**

MaxPatrol 8.

Пилотный проект

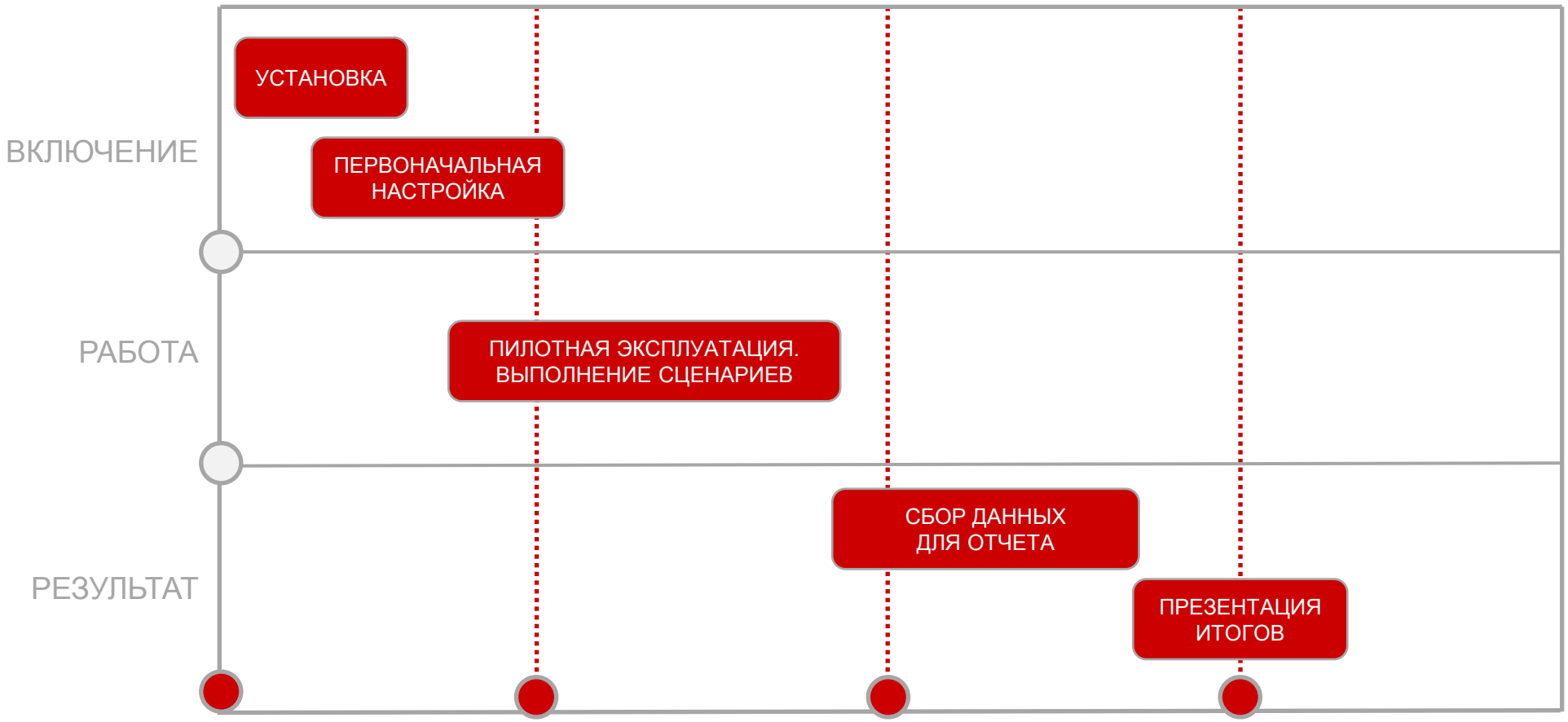
Что нужно для пилота

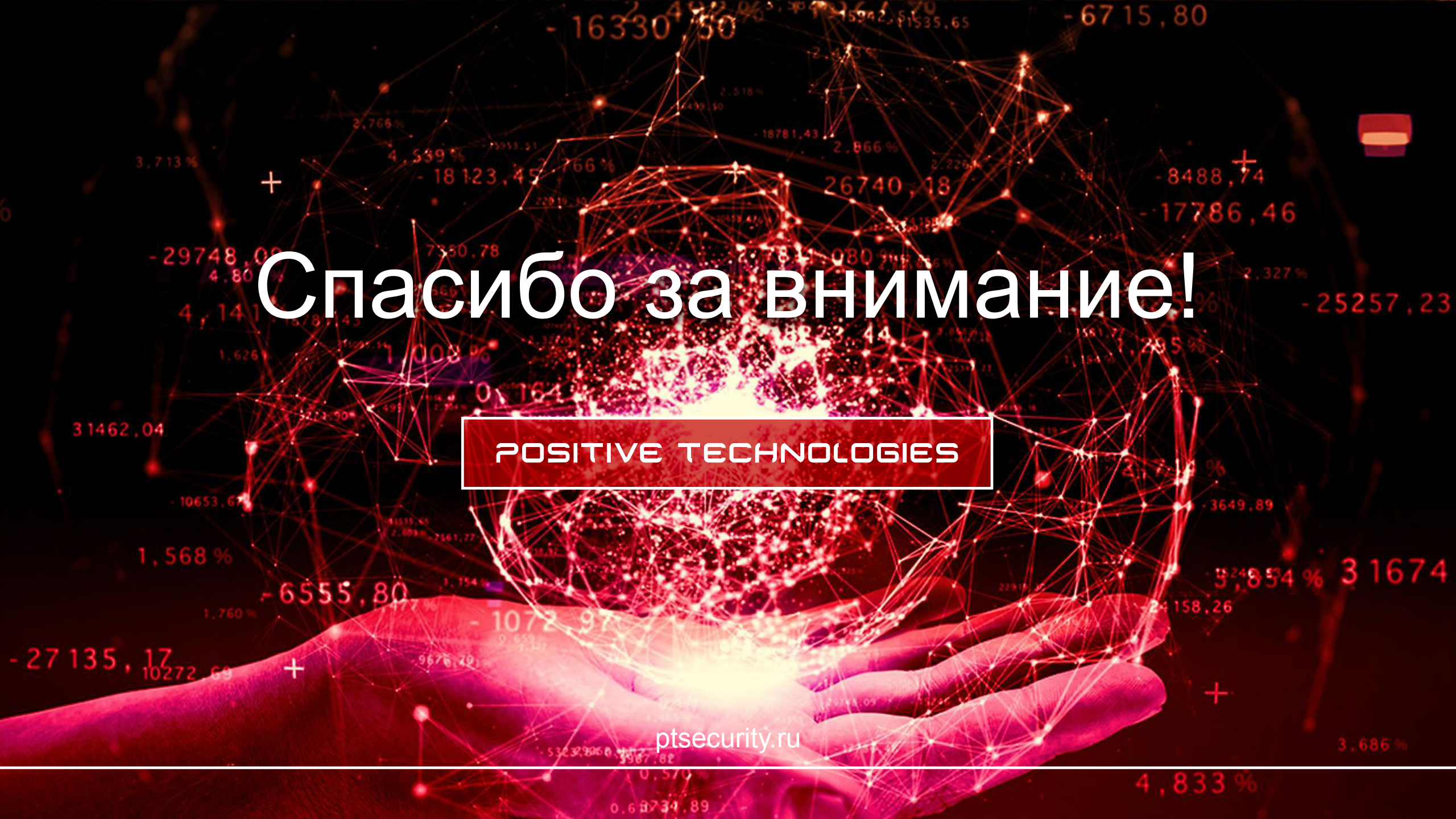
POSITIVE TECHNOLOGIES

- **Полностью** заполнена анкета
- Получено коммерческое и техническое одобрение от PT
- Составлен план пилота
- Назначена дата начала проекта

Примерный план

POSITIVE TECHNOLOGIES




Спасибо за внимание!
POSITIVE TECHNOLOGIES
ptsecurity.ru