MaxPatrol SIEM:
система выявления инцидентов ИБ в реальном времени

POSITIVE TECHNOLOGIES

ptsecurity.com

Как узнать об инциденте?

POSITIVE TECHNOLOGIES

1

Почувствовать!

2

Вас тихо “порадуют”

3

Вас громко “обрадуют”

4

Пригласить экспертов провести аудит

5

Внедрить систему выявления инцидентов ИБ:
инструмент + специалисты + процессы

Почему необходим SIEM?

POSITIVE TECHNOLOGIES

- Средняя компания создает терабайты информации в месяц
- Десятки систем различных типов, информация о сетевой активности и пользователях
- Для качественного выявления инцидентов необходимо анализировать большую часть этой информации

SIEM

- Единая точка контроля ИБ и работы средств СЗИ
- Унификация поступающей информации и её перекрестный анализ в едином интерфейсе
- **Средство выявления и расследования инцидентов ИБ**

Почему еще необходим SIEM

POSITIVE TECHNOLOGIES

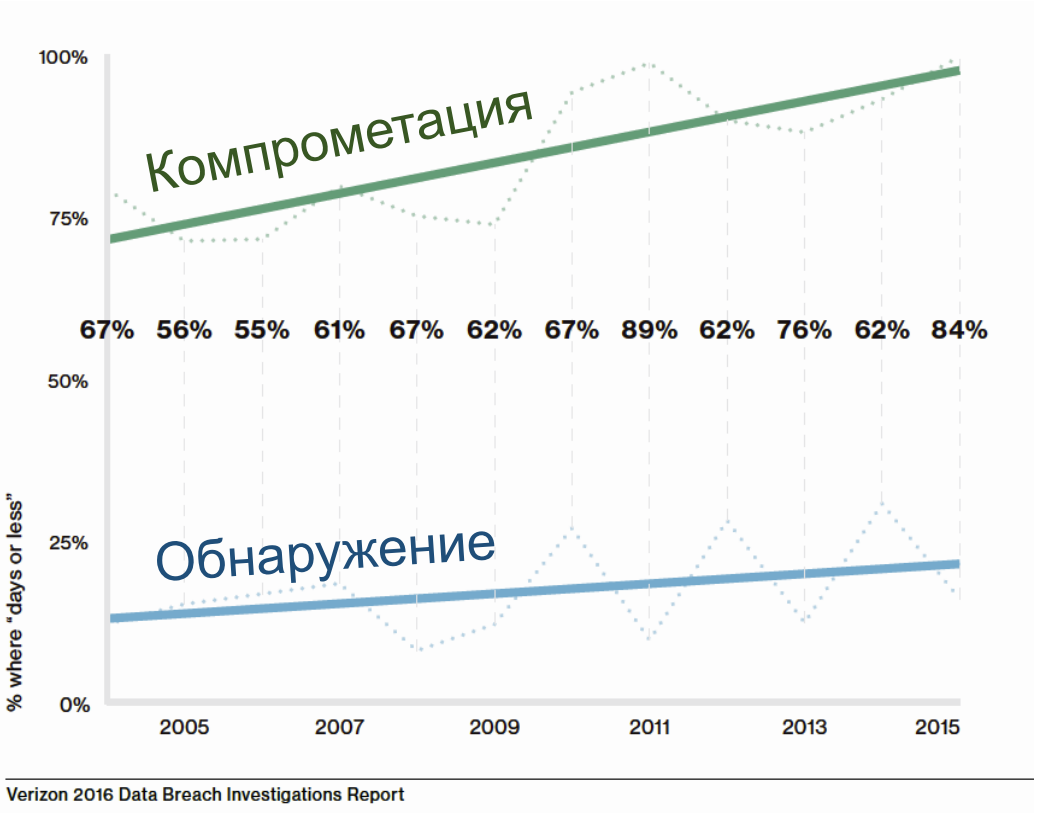
- Инцидент был вчера, а логи только за сегодня
- С рестартом служб перезаписывается лог файл
- Пока смотрели логи, часть уже затерлась
- Когда это было? Какой временной метке верить и кому верить вообще?

Мировая тенденция – разрыв увеличивается

POSITIVE TECHNOLOGIES

Дни, часы, минуты
занимает
компрометация

Недели, месяцы
проходят до
обнаружения



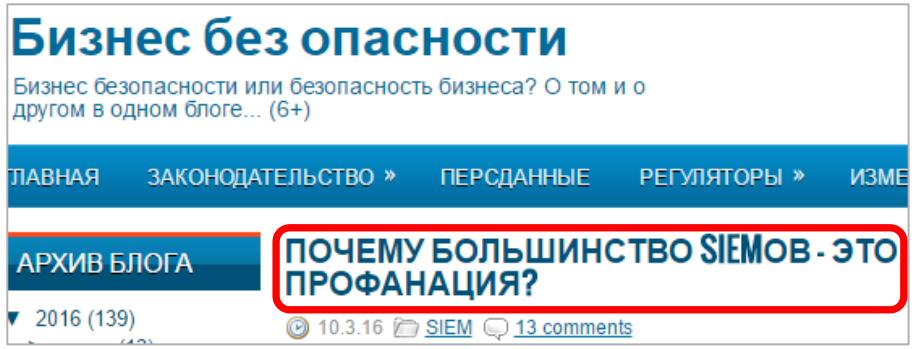
Verizon 2016 Data Breach Investigations Report

- Согласно Netwrix 2014 SIEM Efficiency Survey Report* 74% компаний (из 800 в 30 отраслях), внедривших SIEM, заявили, что SIEM почти не повлияли на число инцидентов безопасности в лучшую сторону
- Согласно 2015 Trustwave Global Security Report** среднее время до обнаружения вторжения/ компрометации составляет 188 дней

* http://www.netwrix.com/download/documents/2014_SIEM_Efficiency_Survey_Report.pdf
** https://www2.trustwave.com/rs/815-RFM-693/images/2015_TrustwaveGlobalSecurityReport.pdf

Проблемы индустрии SIEM: мнения экспертов и аналитиков

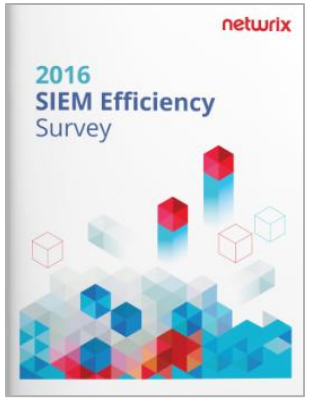
POSITIVE TECHNOLOGIES



Алексей Лукацкий, Эксперт ИБ

Выступление НТЦ «Вулкан» на уральском форуме

- 69% респондентов ищут возможность сократить стоимость SIEM
- Разрастание персонала – причина №1 увеличения стоимости SIEM
- Около 55% респондентов ищут дополнительных сотрудников для работы с SIEM
- Почти 81% респондентов отметили что отчеты SIEM содержат много «шума» (ложных срабатываний). В 2014 году эту проблему отметили лишь 75% респондентов
- При этом 63% респондентов отметили что отчеты SIEM недостаточны



В опросе SIEM Efficiency приняли участие 234 enterprise-компании

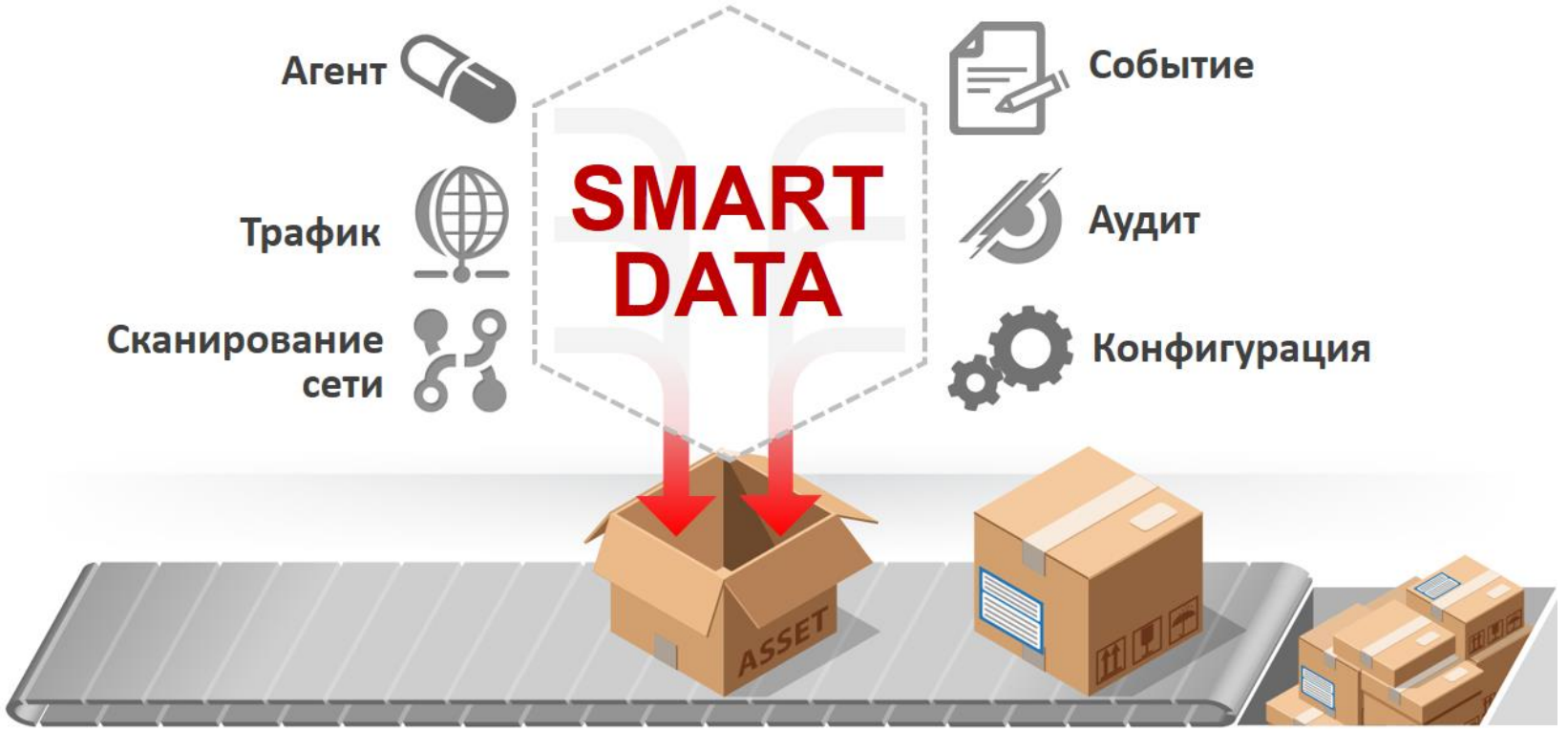
MaxPatrol SIEM: Активоцентрический подход

POSITIVE TECHNOLOGIES

Полная модель инфраструктуры

Платформа MaxPatrol

База знаний PTKB



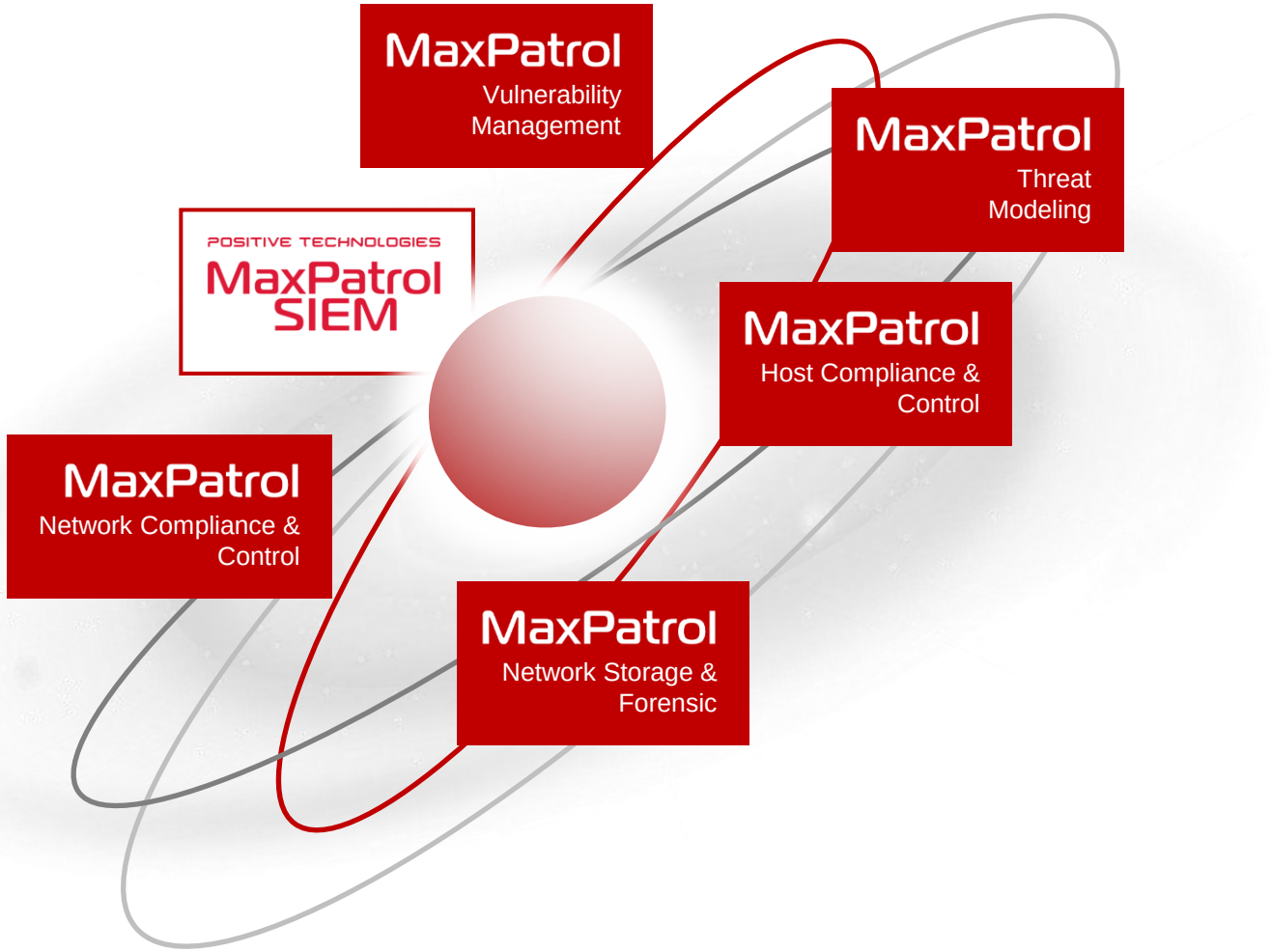
MaxPatrol SIEM: Единая платформа

POSITIVE TECHNOLOGIES

Полная модель инфраструктуры

Платформа MaxPatrol

База знаний PTKB



Поддержка источников

– 100 –

– 200 –

– 400 –

MaxPatrol SIEM: Сбор данных с конечных точек

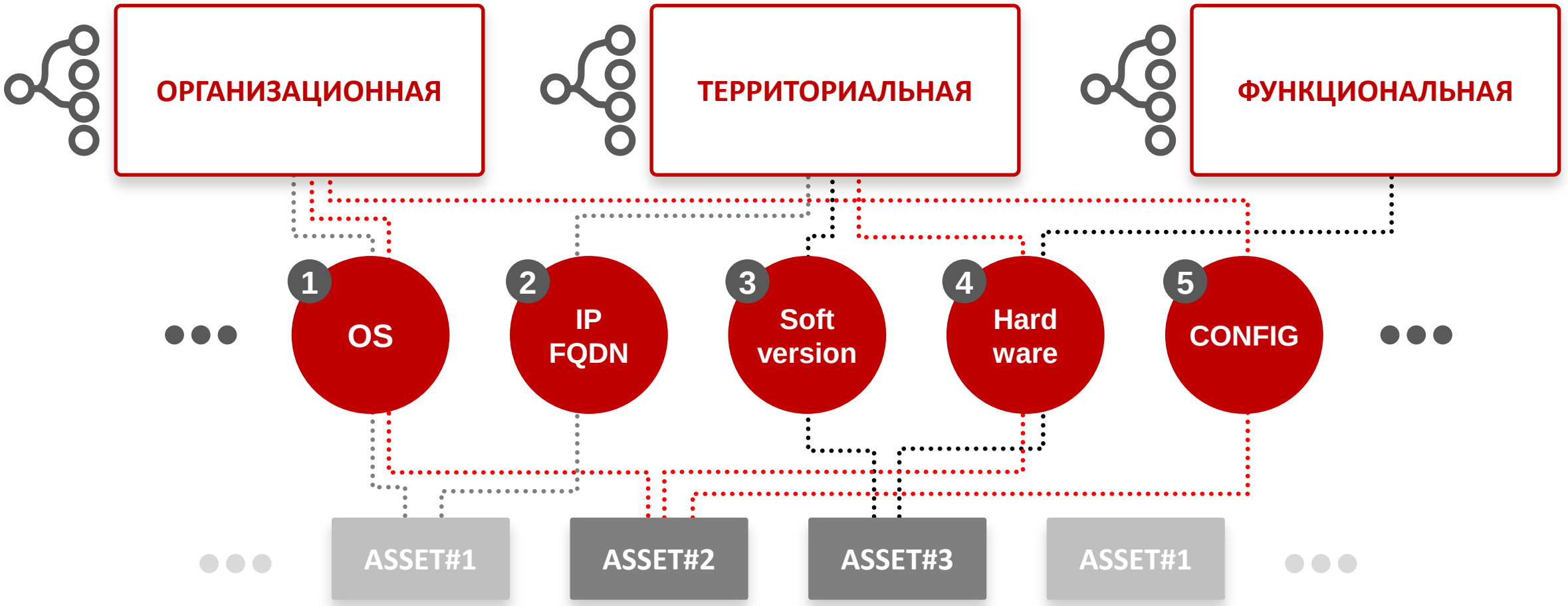
POSITIVE TECHNOLOGIES

Endpoint-агент для контроля:

- Служб, сервисов, процессов
- Файловой активности
- Действий пользователей
- Сетевой активности

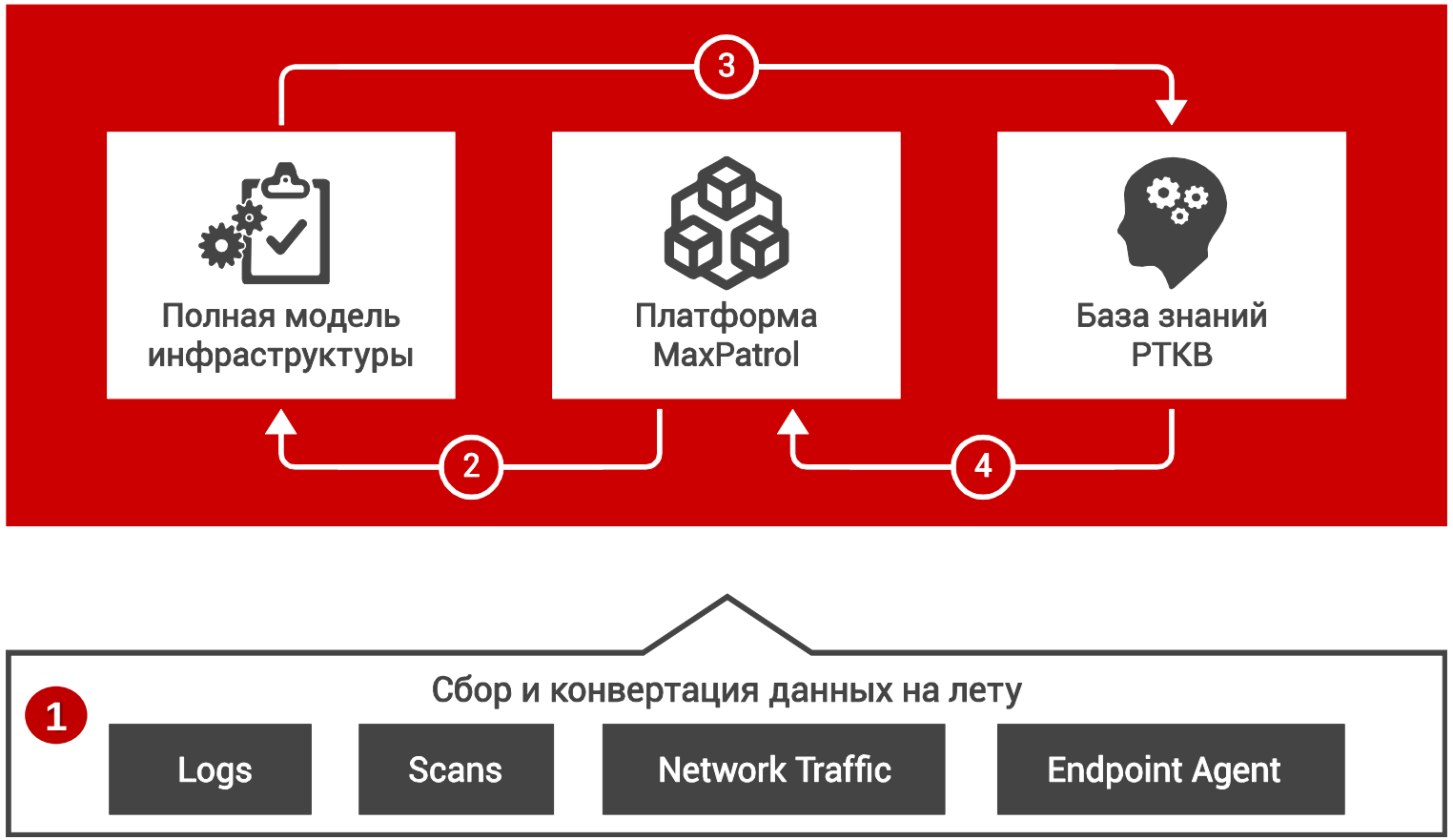
MaxPatrol SIEM: Управление активами

POSITIVE TECHNOLOGIES



MaxPatrol SIEM: Как это работает всё вместе

POSITIVE TECHNOLOGIES



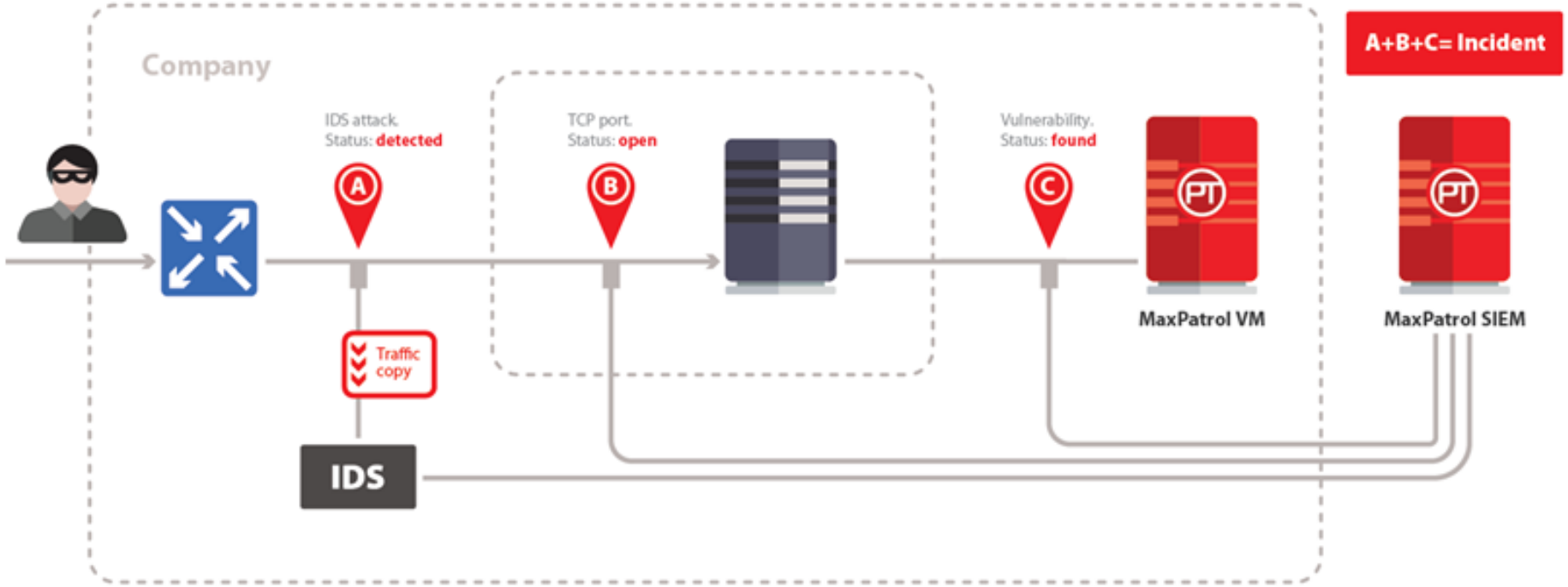
MaxPatrol SIEM: Модельные корреляции

POSITIVE TECHNOLOGIES

Полная модель инфраструктуры

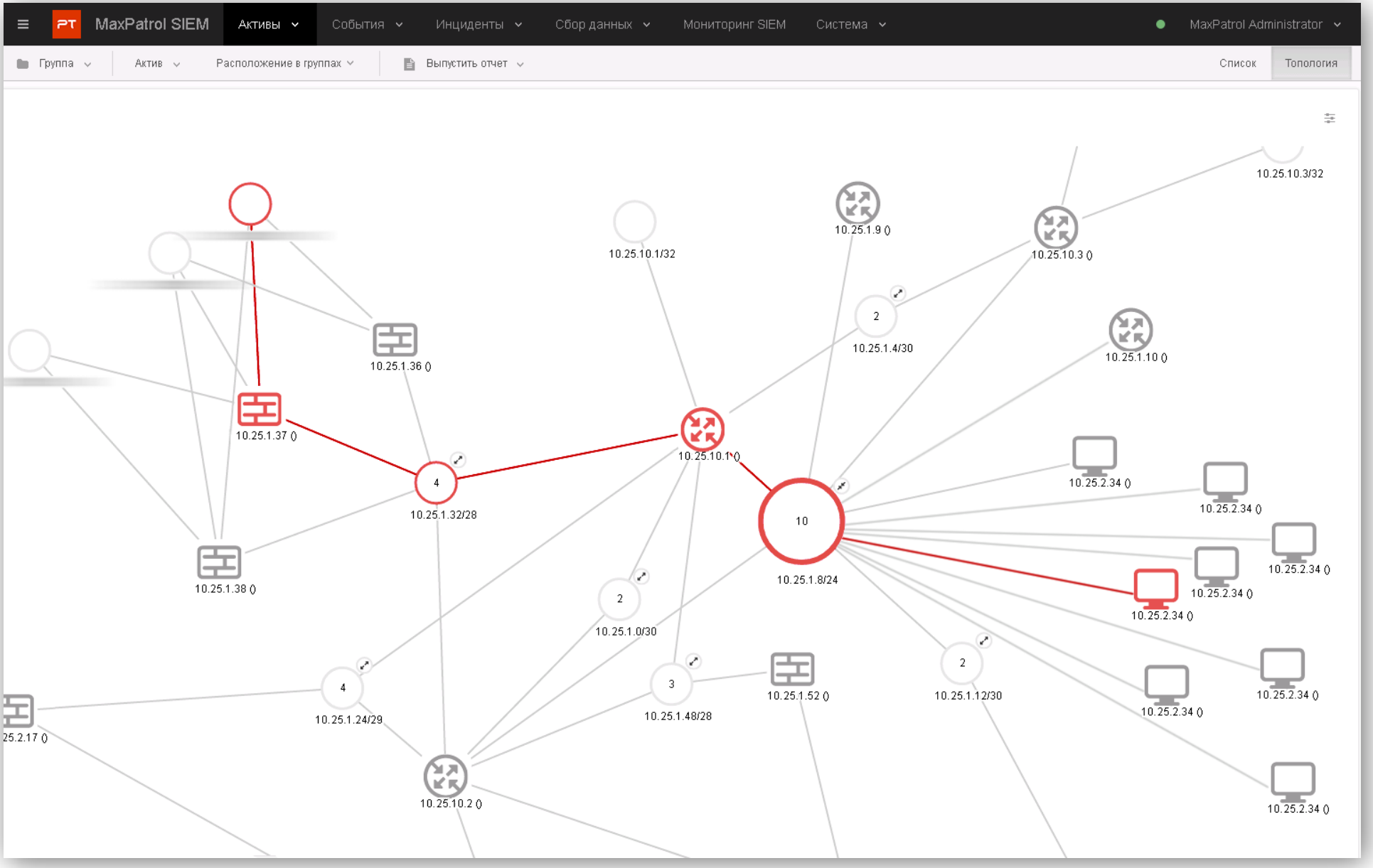
Платформа MaxPatrol

База знаний PTKB



MaxPatrol SIEM: Топология сети

POSITIVE TECHNOLOGIES



MaxPatrol 8

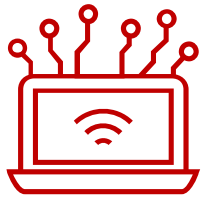
POSITIVE TECHNOLOGIES

ptsecurity.ru

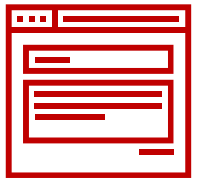
Почему инфраструктура уязвима

POSITIVE TECHNOLOGIES

Слабые пароли



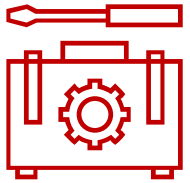
Небезопасные беспроводные сети



Уязвимости веб-приложений

Программное обеспечение

Социальная инженерия



Ошибки в настройках:

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

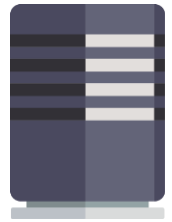
Процесс управления уязвимостями

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

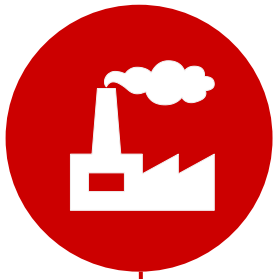
продукт года в категории **Vulnerability Management** по версии британской премии **Cyber Security Awards 2016**

Дополнительные сценарии

POSITIVE TECHNOLOGIES

ERP

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



АСУ ТП

- SIEMENS
- invensys
- Rockwell Automation
- Schneider Electric

ТЕЛЕКОМ

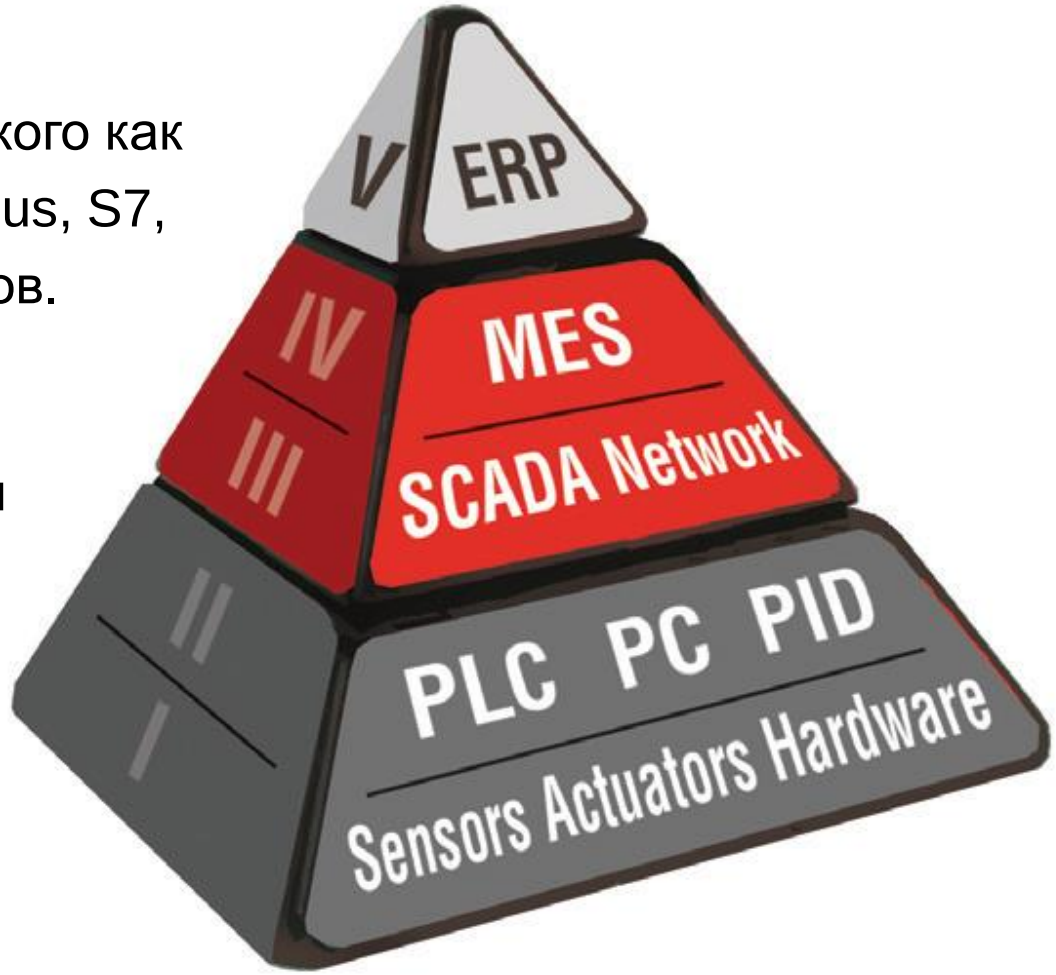
- HUAWEI
- ERICSSON

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.

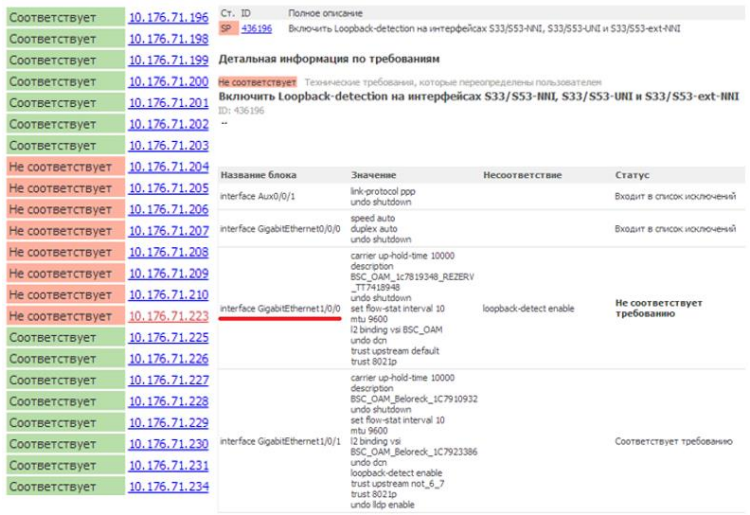
База знаний содержит более **30 000** проверок на уязвимости и требования по безопасности для *HMI/SCADA, PLC, RTU* ведущих производителей: **Siemens, Schneider Electric, Rockwell Automation, ABB.**



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

--

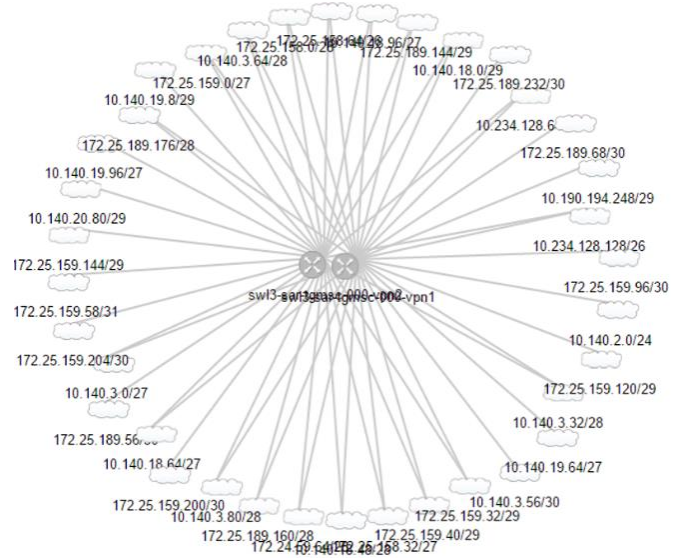
Название блока	Значение	Несоответствие	Статус
interface Aux0/0/1	link-protocol ppp undo shutdown		Входит в список исключений
interface GigabitEthernet0/0/0	speed auto duplex auto undo shutdown		Входит в список исключений
interface GigabitEthernet1/0/0	carrier up-hold-time 10000 description BSC_OAM_1c7819348_REZERV_TT7418948 undo shutdown set flow-stat interval 10 mtu 9600 l2 binding vsi BSC_OAM undo dcn trust upstream default trust 802.1p	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 802.1p 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®

Схема работы

POSITIVE TECHNOLOGIES

РЕСУРСЫ

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

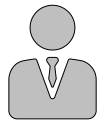
PCI DSS, ISO 27001,
Персональные данные

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

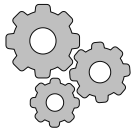
Корпоративные стандарты

ОТЧЕТНОСТЬ



УПРАВЛЕНЧЕСКАЯ

АНАЛИТИЧЕСКАЯ



ТЕХНИЧЕСКАЯ

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

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

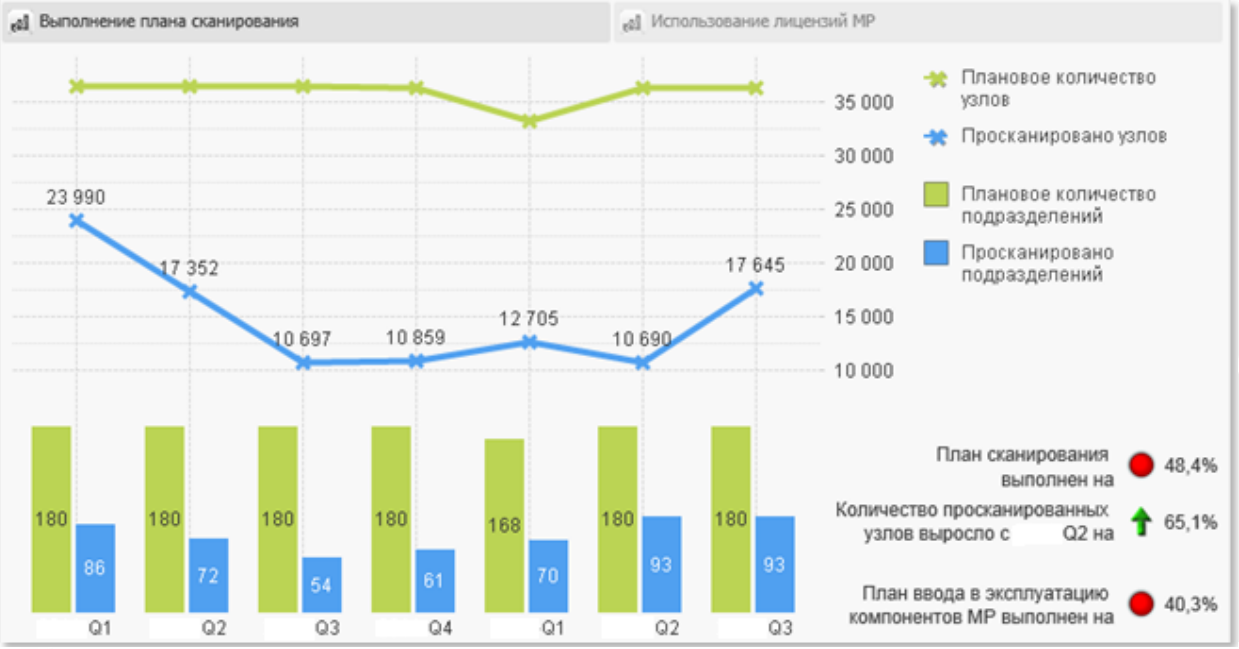
Количество узлов с запрещенным ПО	3,7%
Количество узлов с обязательным ПО	16,7%
Соблюдение лицензионной политики	---
Использование запрещенного оборудования	---

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


Спасибо!
POSITIVE TECHNOLOGIES
Контакты:
marketing@DialogNauka.ru
8 (495) 980-67-76
ptsecurity.ru