Positive Technologies

MaxPatrol 8

Контроль состояния защищённости как механизм защиты

Алексей Голдбергс

POSITIVE TECHNOLOGIES

SecurITy conference

Источники уязвимостей

- Ошибки в веб-приложениях
- Небезопасные беспроводные сети
- Случайные ошибки в настройках:
  - сетевого оборудования
  - систем защиты периметра
  - веб-приложений
  - баз данных
- Программные средства сторонней разработки
- Слабые пароли

Управление уязвимостями

Ключевые возможности

Инвентаризация и детализированная проверка

Комплексная оценка защищенности

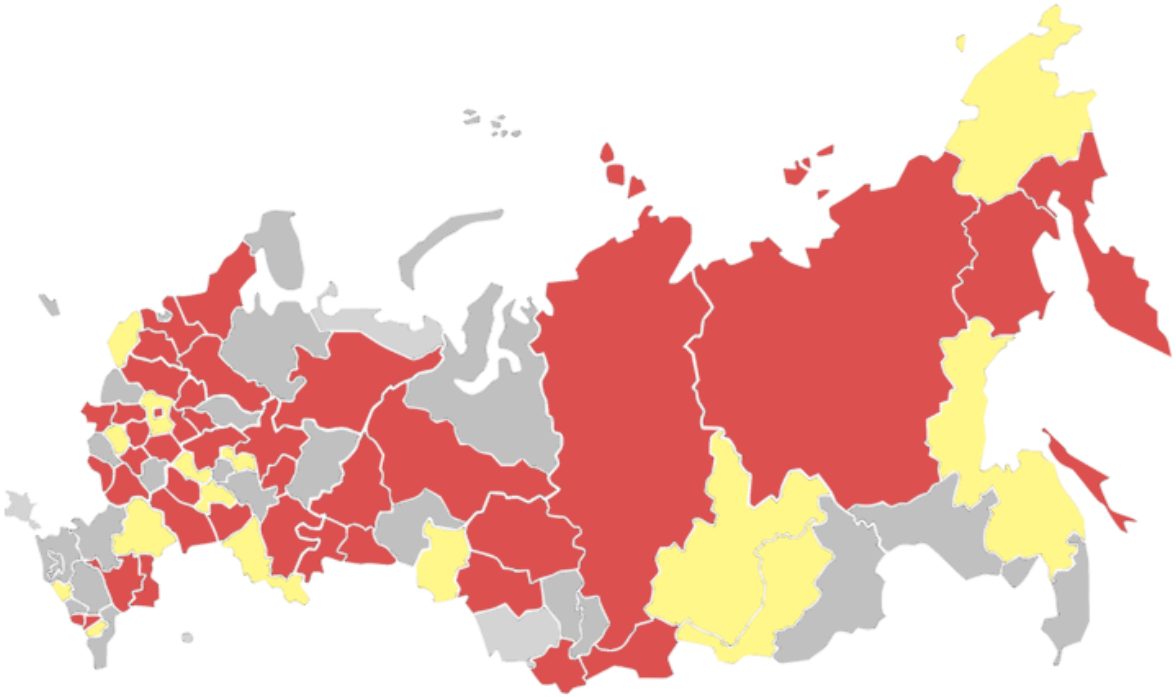
Ежедневно обновляемая база знаний

Постоянный контроль соответствия

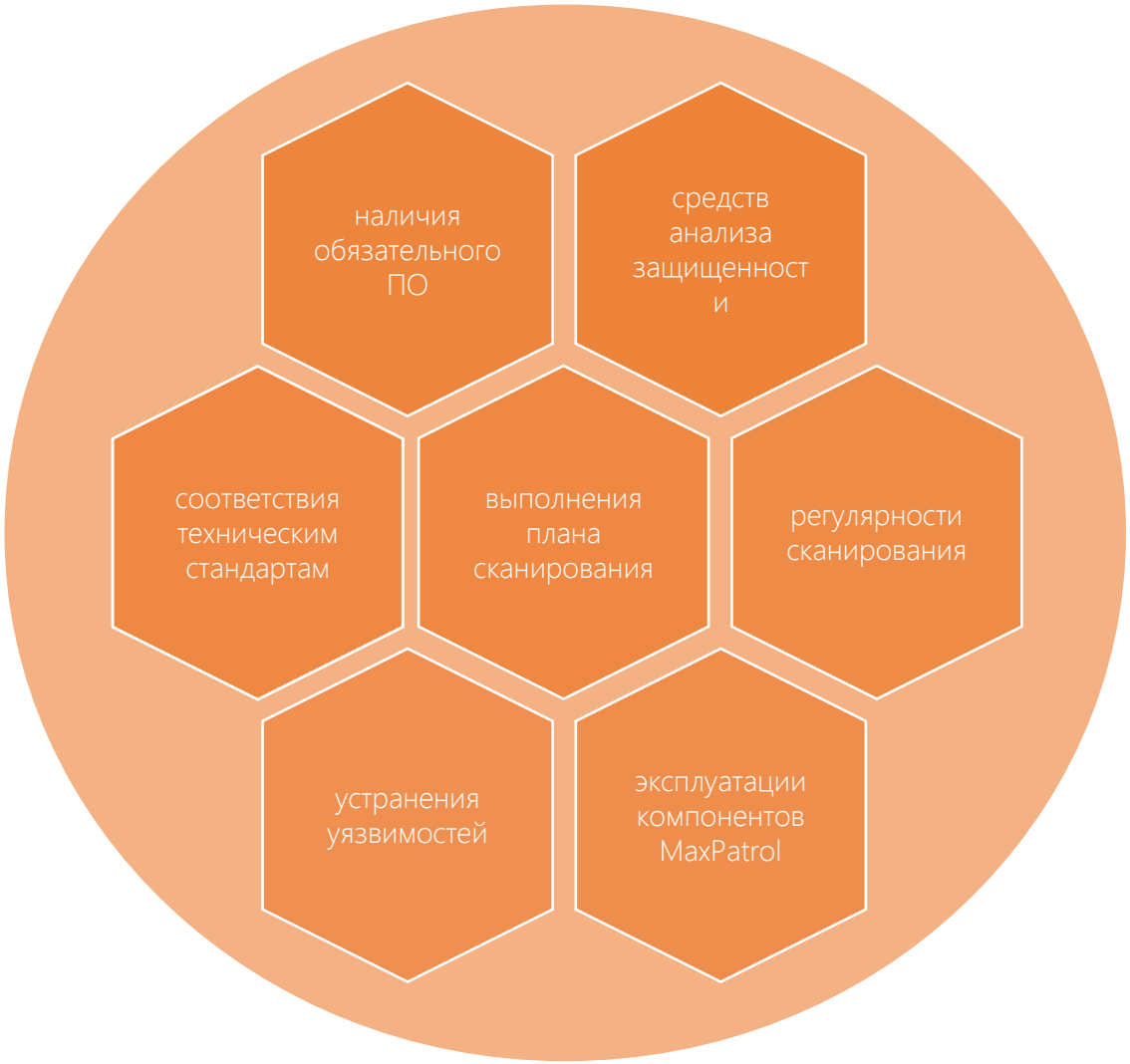
Технические и высокоуровневые отчеты

Портал аналитической отчетности

Business Intelligence система для оперативного анализа и представления данных о состоянии защищенности информационных и телекоммуникационных систем



Контроль эффективности процессов ИБ



Управление угрозами ИБ

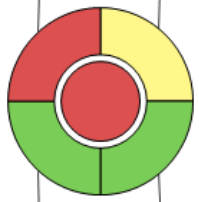
Показатели информационной безопасности инфраструктуры за 2013-Q1

Контроль защищенности

Обнаружено High уязвимостей	4,0%
Обнаружено Medium уязвимостей	43,7%
Количество уязвимостей меньше, чем в 2012-Q4, на	-37,7%
Количество узлов с High уязвимостями	6,3%
Количество узлов с Medium уязвимостями	47,2%
Количество уязвимых узлов уменьшилось с 2012-Q4 на	-24,8%
Среднее количество High уязвимостей на узел	0,07
Среднее количество Medium уязвимостей на узел	0,79

Управление активами

Количество узлов с запрещенным ПО	6,6%
Количество узлов без обязательного к установке ПО	88,0%



Контроль эффективности ИБ

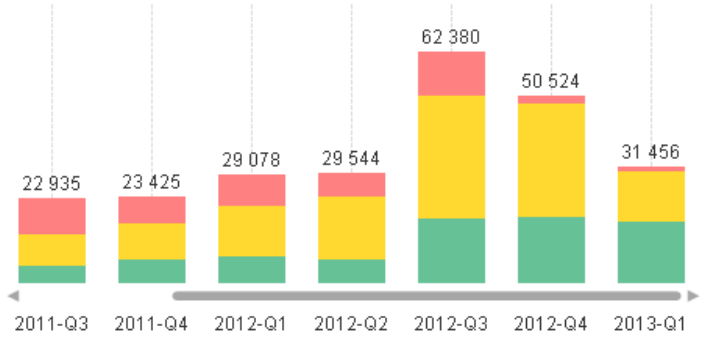
Устранено уязвимостей	41,5%
План сканирования узлов выполнен на	69,1%
Количество просканированных узлов выросло с 2012-Q4 на	3,0%
Заданная регулярность сканирования узлов соблюдена на	97,1%
План ввода в эксплуатацию компонентов MP выполнен на	39,8%

Соответствие стандартам

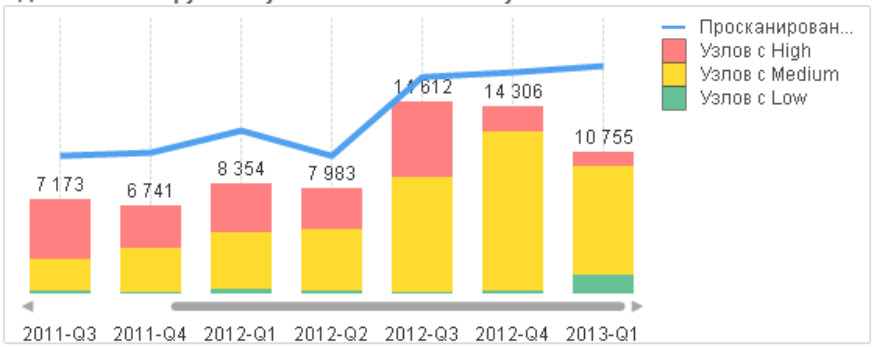
Узлы, соответствующие стандартам	21,2%
Количество соответствующих узлов изменилось на	-50,1%
Количество соответствий требованиям	96,9%
Количество соответствий требованиям изменилось на	9,8%

Динамика изменения состояния защищенности

Динамика обнаружения уязвимостей

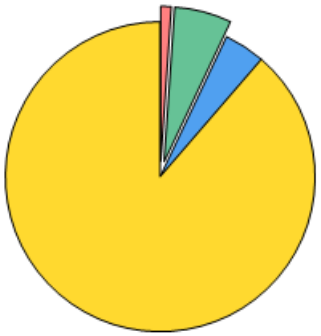


Динамика обнаружения узлов с максимальной уязвимостью



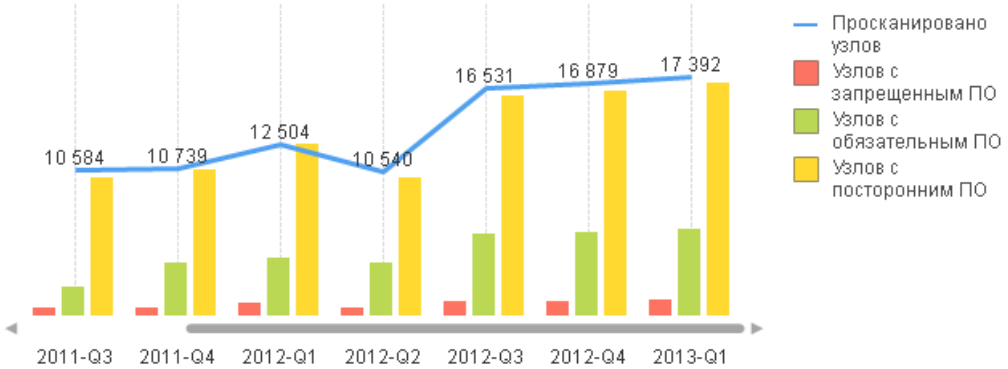
Наглядные метрики

Установленное программное обеспечение

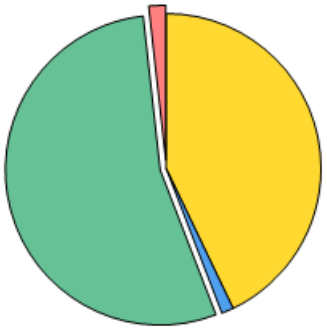


Запрещенное	1,08%
Обязательное	5,96%
Поддерживаемое	4,28%
Постороннее	88,68%

Всего экземпляров обнаруженного ПО:	105 242
Запрещенного:	1 141
Обязательного:	6 272
Поддерживаемого:	4 503
Постороннего:	93 326



Уязвимости установленного ПО



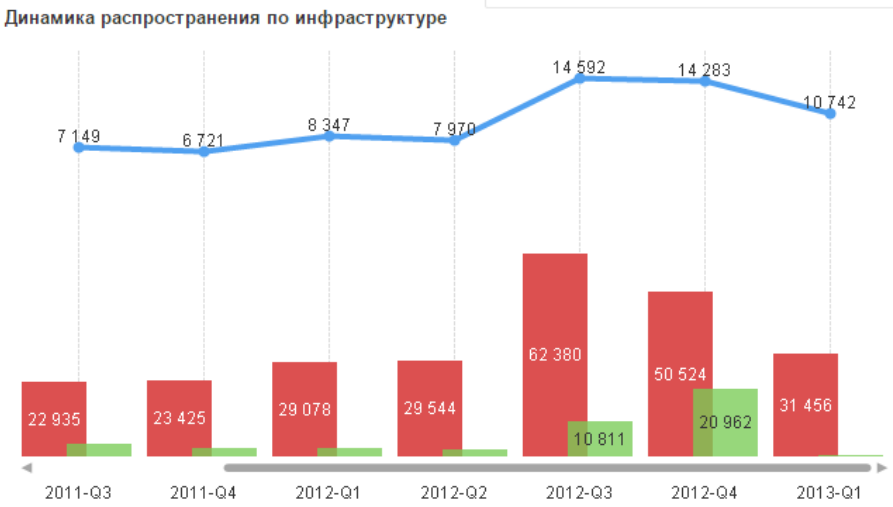
Запрещенное	494
Обязательное	15 191
Поддерживаемое	349
Постороннее	12 044

Установка обязательного ПО

Установлено обязательного ПО: 12,1%

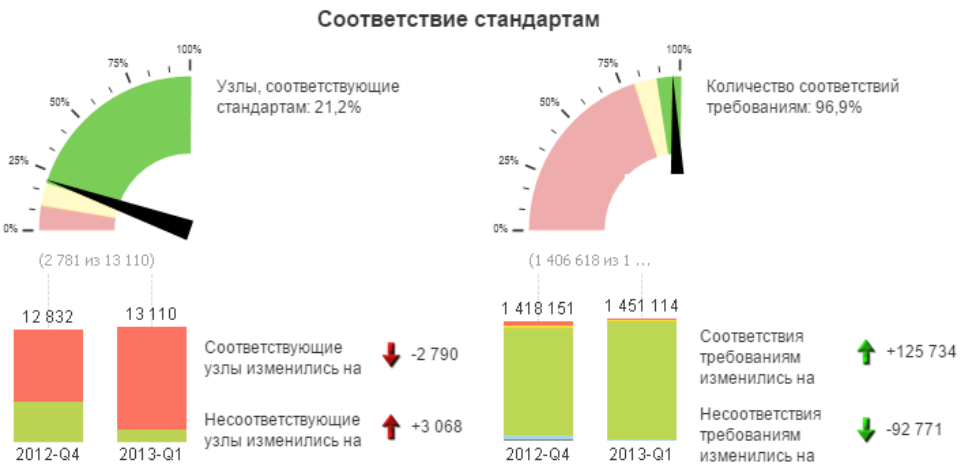
Регион / Подразделение / Узел	Microsoft RDP	SSH	Антивирус Касперского
Региональное отделение по Калужской области	89,81%	8,33%	0,00%
Региональное отделение по Республике Башкортоста	**89,74%**	**0,00%**	**0,00%**
Филиал №18 по Республике Башкорто	94,44%	0,00%	0,00%
Региональное отделение по Республик	85,71%	0,00%	0,00%
Региональное отделение по Новосибирской области	86,34%	0,00%	0,00%
Региональное отделение по Удмуртской Республике	71,43%	14,29%	0,00%
Региональное отделение по Камчатскому краю	77,78%	5,56%	0,00%
Региональное отделение по Республике Калмыкия	75,47%	3,77%	0,00%
Региональное отделение по Владимирской области	77,65%	0,00%	0,00%
Региональное отделение по Московской области	75,18%	1,17%	0,00%
Региональное отделение по Челябинской области	68,89%	6,67%	0,00%
ЦОД № 3	**75,00%**	**0,00%**	**0,00%**

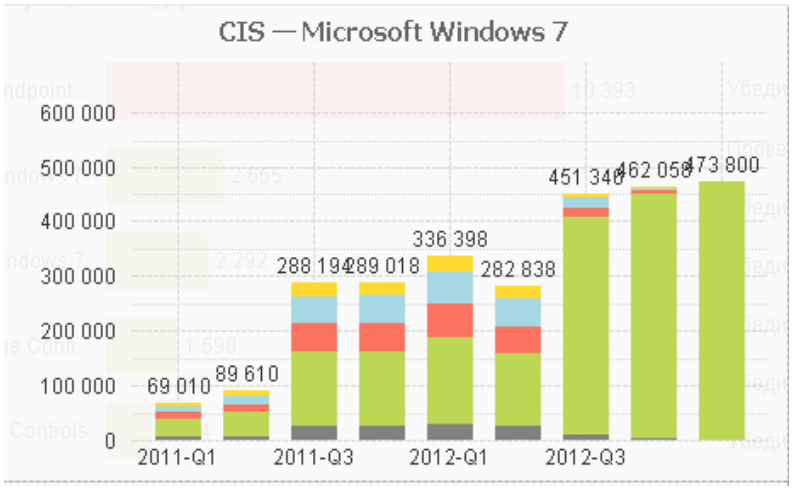
Представление результатов



Самые распространенные уязвимости

Уровень	Уязвимость	Узлов	Оценка CVSS
High	Уязвимость протокола удаленного рабо...	366	6,9
High	Учетная запись пользователя	145	10
High	Уязвимость RPC делает возможной атак...	140	7,8
High	Удаленное управление реестром	72	6,8
High	Отказ в обслуживании при проверке SMB	42	4,8
High	Удаленное выполнение кода при перепо...	41	6,1
High	Найдены учётные записи	37	8,7
High	Стандартный пароль пользователя SYSD...	28	10
High	Подмена диспетчера очереди печати	28	6,9
High	Найден пароль	26	10
High	Найден пароль	26	10





Спасибо!

POSITIVE TECHNOLOGIES

ptsecurity.com