Решения Positive Technologies для коммерческих преприятий

Логинов Роман
Менеджер по продвижению продуктов

ptsecurity.com

POSITIVE TECHNOLOGIES

О компании Positive Technologies

POSITIVE TECHNOLOGIES

200+
аудитов безопасности корпоративных систем

200+
обнаруженных уязвимостей нулевого дня

Главные продукты

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

Визионер 2017
WAF Magic Quadrant
Gartner®

16 **лет исследований и экспертизы**

150+ уязвимостей нулевого дня в системах SCADA

50+ расследований взломов инфраструктуры

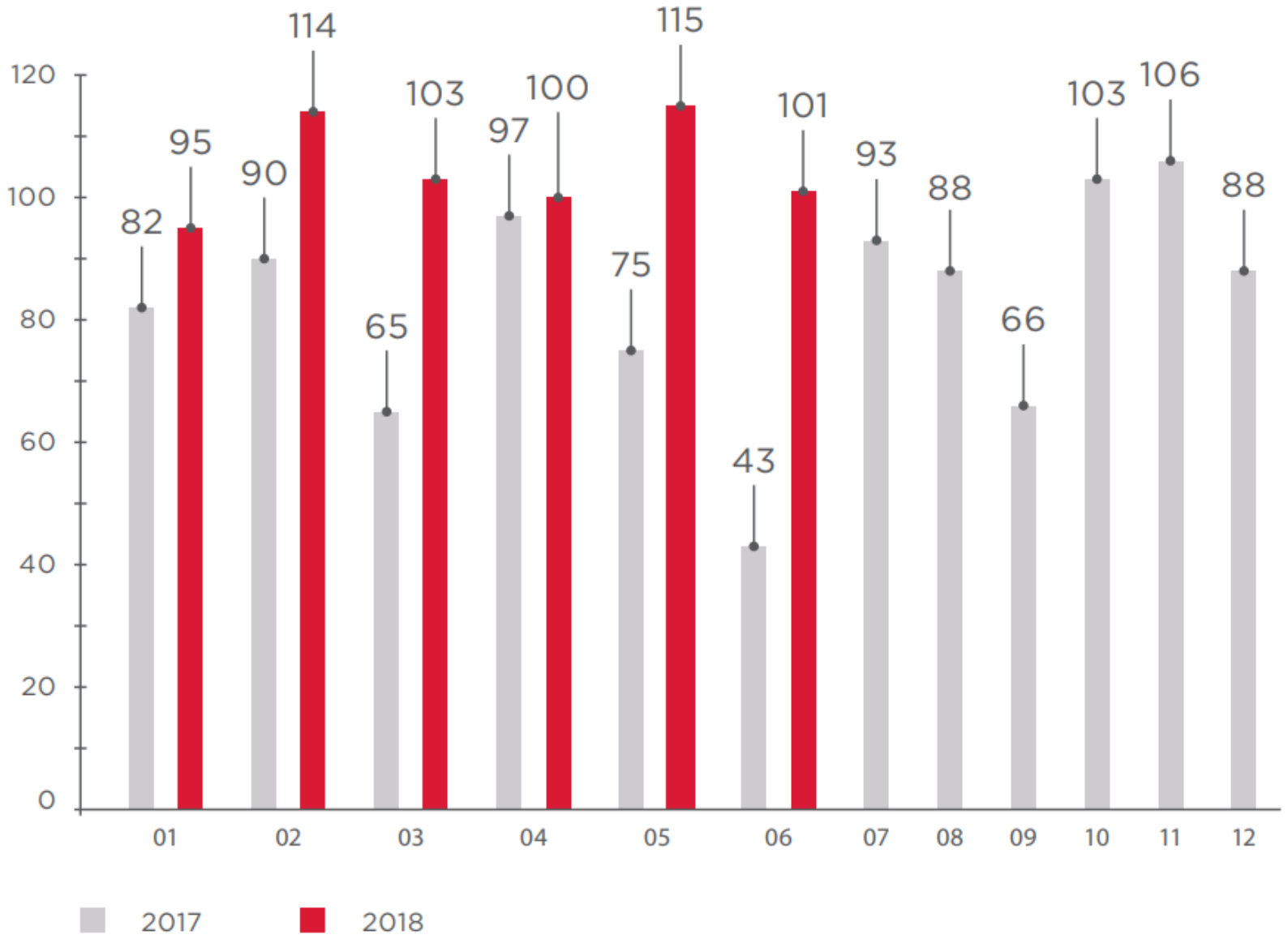
500+ исследований безопасности мобильных и веб-приложений

Из новенького

POSITIVE TECHNOLOGIES

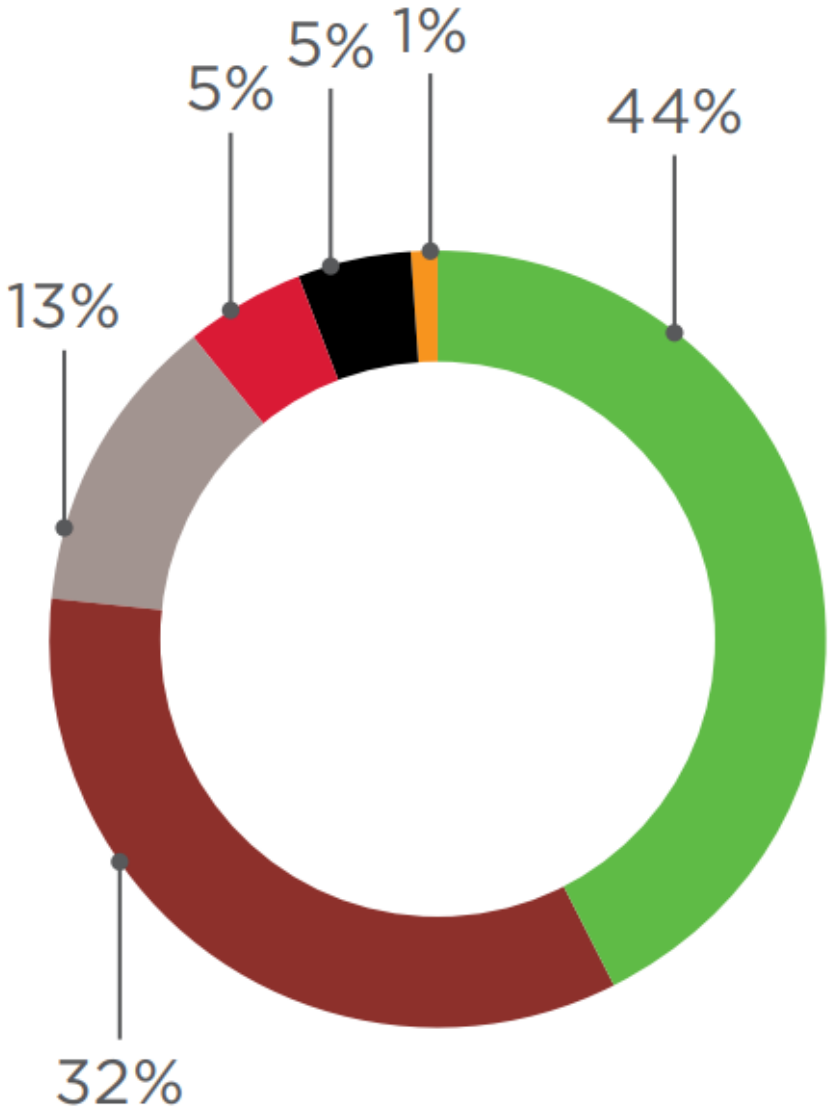
Динамика атак

POSITIVE TECHNOLOGIES



Объекты атак

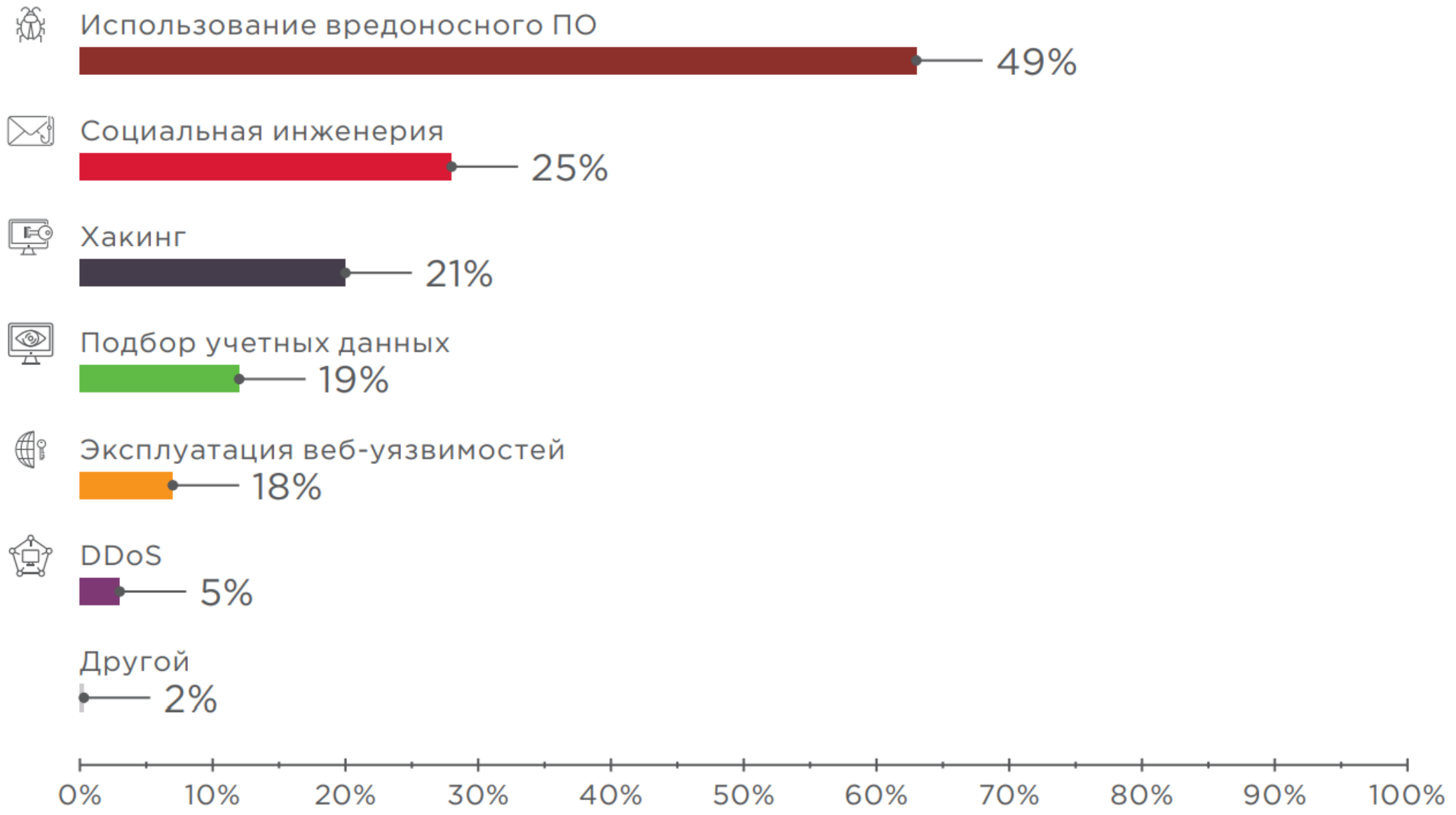
POSITIVE TECHNOLOGIES



- Инфраструктура
- Веб-ресурсы
- Пользователи
- Мобильные устройства
- IoT
- Банкоматы и POS-терминалы

Методы атак

POSITIVE TECHNOLOGIES



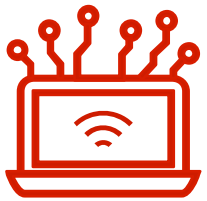
MaxPatrol 8

Контроль защищенности и соответствия стандартам

Почему инфраструктура уязвима

POSITIVE TECHNOLOGIES

Слабые пароли



Небезопасные беспроводные сети

Уязвимости веб-приложений

Программное обеспечение

Социальная инженерия

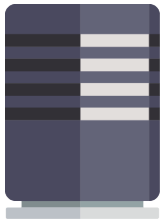
Ошибки в настройках:

- 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

Схема работы

POSITIVE TECHNOLOGIES

РЕСУРСЫ

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

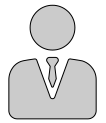
PCI DSS, ISO 27001,
Персональные данные

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

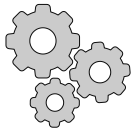
Корпоративные стандарты

ОТЧЕТНОСТЬ



УПРАВЛЕНЧЕСКАЯ

АНАЛИТИЧЕСКАЯ

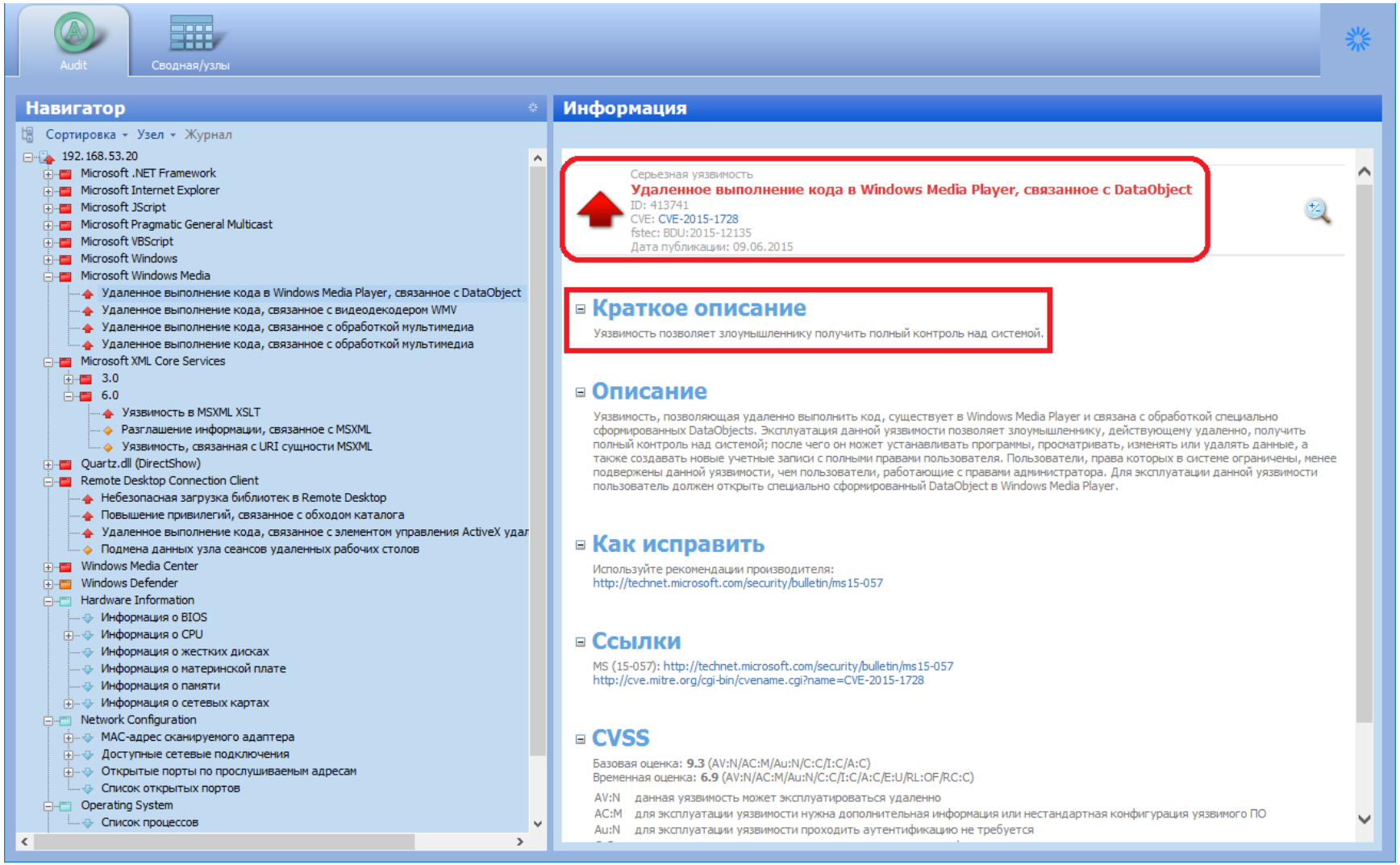


ТЕХНИЧЕСКАЯ

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

Режим Audit (скриншот)

POSITIVE TECHNOLOGIES



Встроенные отчеты

POSITIVE TECHNOLOGIES

MAXPATROL 06.03.2017 17:53:13

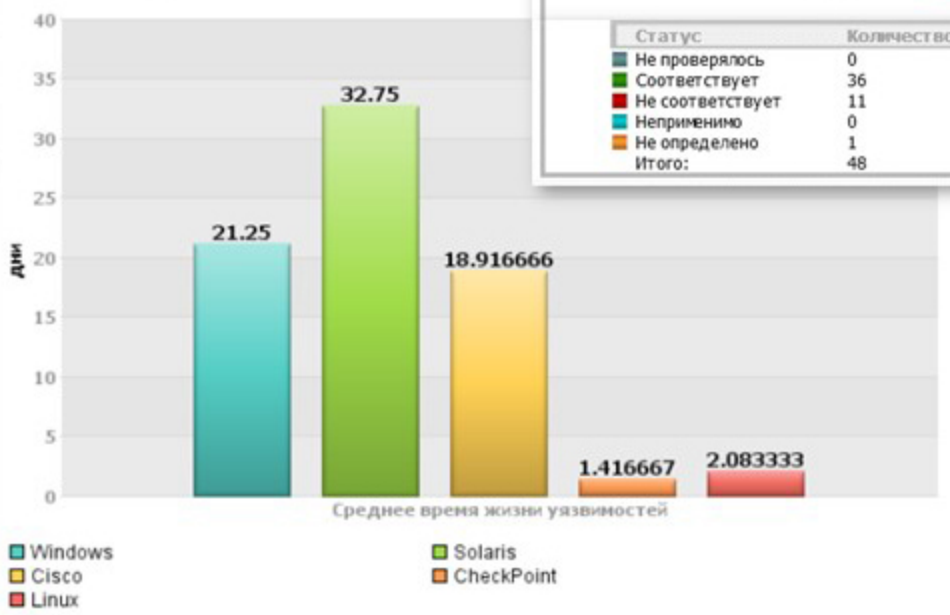
Рейтинг уязвимостей

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

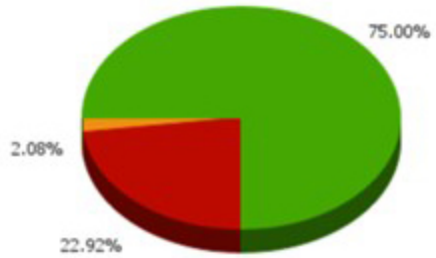


MAXPATROL 06.03.2017 17:53:13

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%

MaxPatrol SIEM

Выявление инцидентов ИБ в реальном времени

Растет разрыв между моментом компрометации и обнаружением

POSITIVE TECHNOLOGIES

62% результативных атак являются целевыми

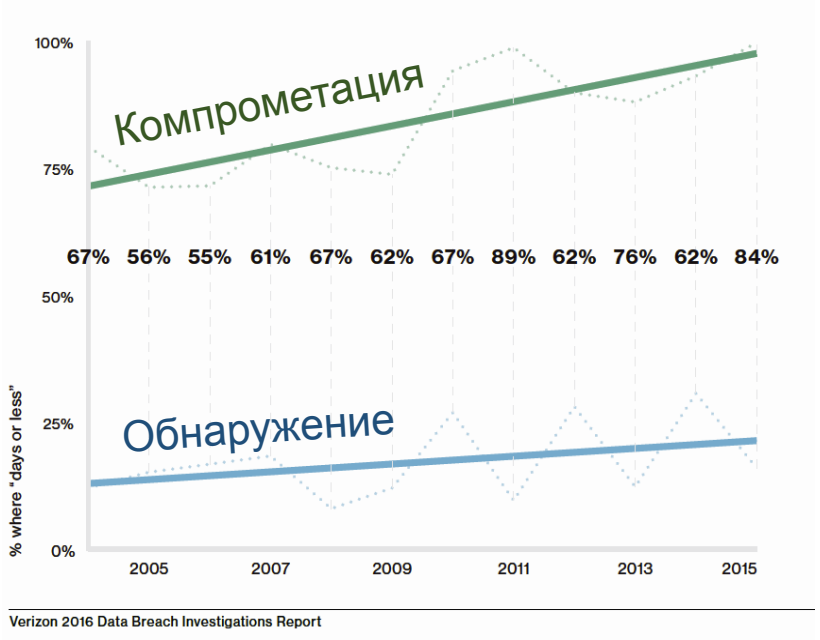
3 года в среднем злоумышленник присутствует в системе

10% атак выявляются самими жертвами

Источник: Кибербезопасность 2016–2017: от итогов к прогнозам (Positive Technologies)

Дни, часы, минуты
занимает компрометация

Недели, месяцы
проходят до обнаружения



MaxPatrol SIEM отвечает на современные вызовы

POSITIVE TECHNOLOGIES

MaxPatrol SIEM

- Контролирует состояние IT-инфраструктуры в любой момент времени.
- Выявляет инциденты даже после изменений IT-ландшафта.
- Автоматически поставляет ИБ-экспертизу в продукт, выявляет новые угрозы и помогает расследовать инциденты.

MaxPatrol SIEM: точная модель IT-инфраструктуры

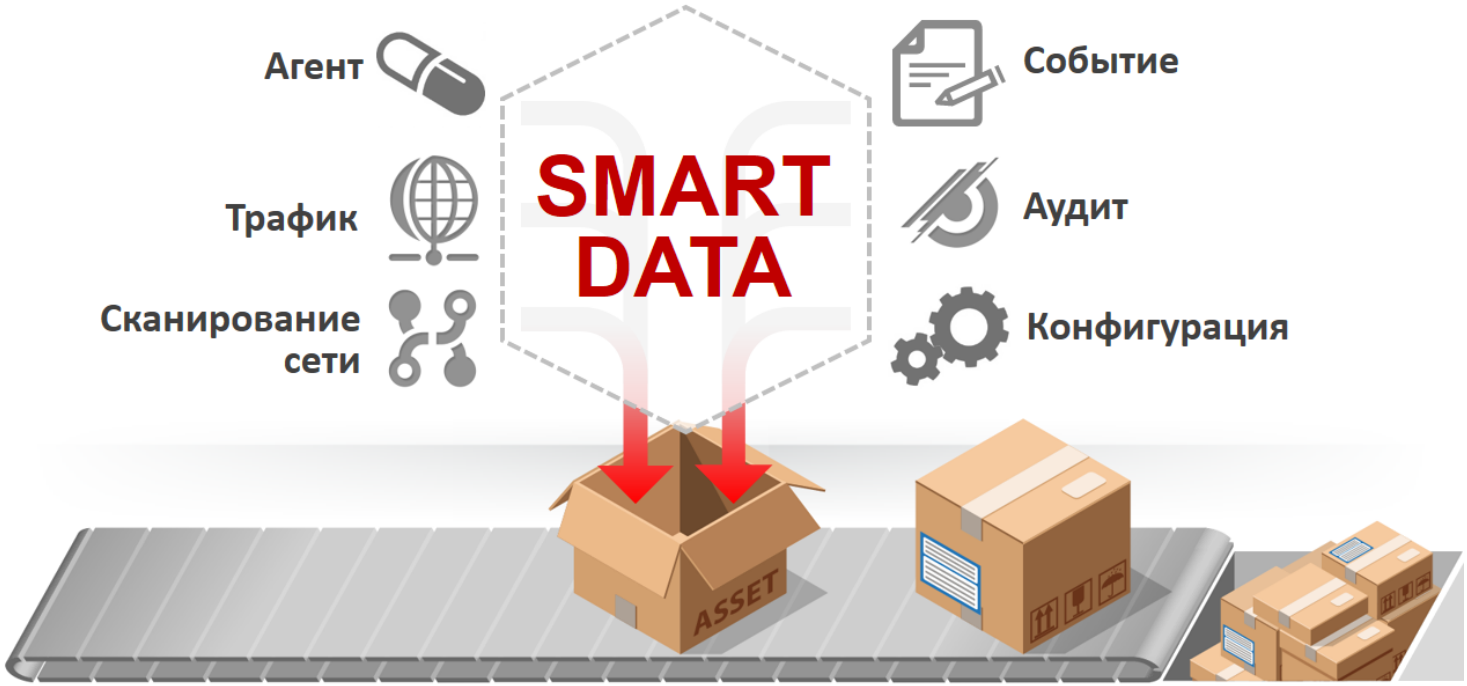
POSITIVE TECHNOLOGIES

Контроль IT-инфраструктуры

- Автоматически строит полную модель IT-инфраструктуры.
- Постоянно обогащается новыми данными об IT-активах.
- Автоматически идентифицирует IT-активы даже после изменения IP- и MAC-адреса и других характеристик.

Адаптация к изменениям

Профилактика угроз



MaxPatrol SIEM: полная и точная модель IT-активов

POSITIVE TECHNOLOGIES

Контроль IT-инфраструктуры

Адаптация к изменениям

Профилактика угроз

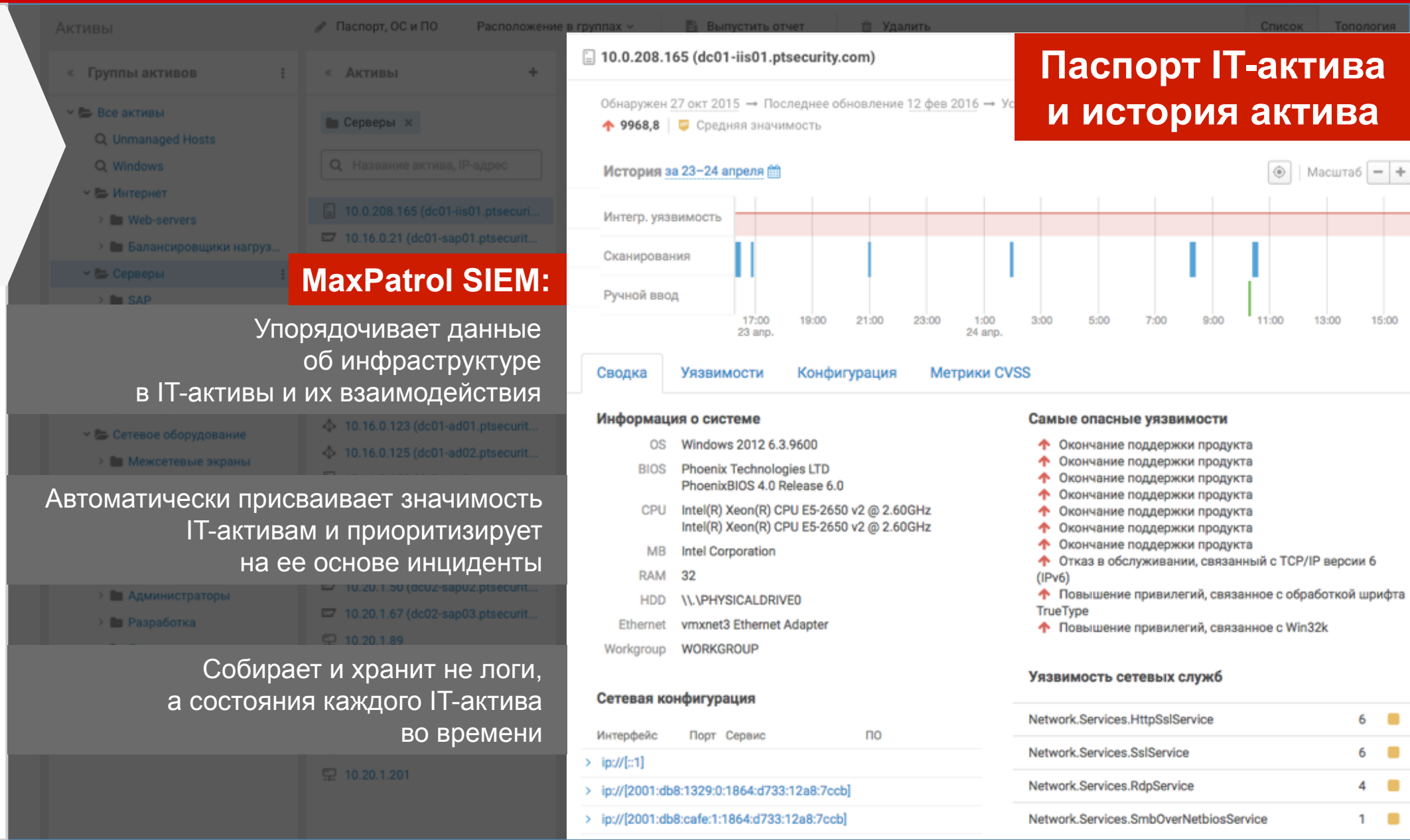
MaxPatrol SIEM:

Упорядочивает данные об инфраструктуре в IT-активы и их взаимодействия

Автоматически присваивает значимость IT-активам и приоритизирует на ее основе инциденты

Собирает и хранит не логи, а состояния каждого IT-актива во времени

Паспорт IT-актива и история актива



MaxPatrol SIEM: сетевая достижимость

POSITIVE TECHNOLOGIES

Контроль IT-инфраструктуры

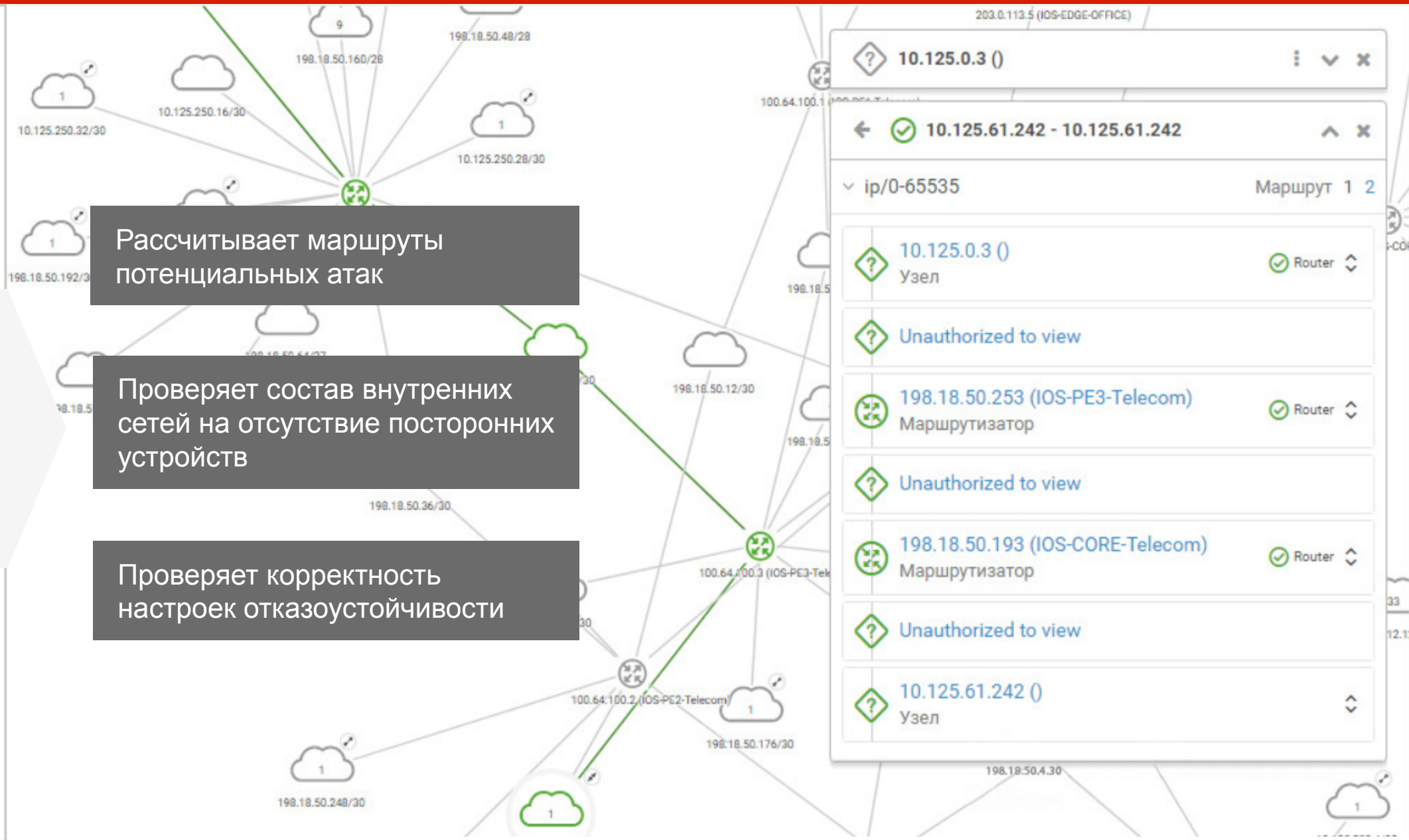
Адаптация к изменениям

Профилактика угроз

Рассчитывает маршруты потенциальных атак

Проверяет состав внутренних сетей на отсутствие посторонних устройств

Проверяет корректность настроек отказоустойчивости



MaxPatrol SIEM: модельные корреляции

POSITIVE TECHNOLOGIES

Контроль IT-инфраструктуры

Адаптация к изменениям

Профилактика угроз

MaxPatrol SIEM автоматически адаптируется к изменениям IT-ландшафта.

Создает корреляции на основе данных IT-активов и динамических групп активов, а не логов.

Правила корреляции продолжают выявлять угрозы после появления нового оборудования или изменения конфигурации сетевых узлов.

MaxPatrol SIEM: в каждом пакете обновлений PT KB

POSITIVE TECHNOLOGIES

Контроль
IT-инфраструктуры

Адаптация
к изменениям

**Профилактика
угроз**

Новые правила
корреляции, агрегации,
нормализации

Рекомендации по сбору
информации из MP SIEM
для подтверждения инцидента
и его расследования

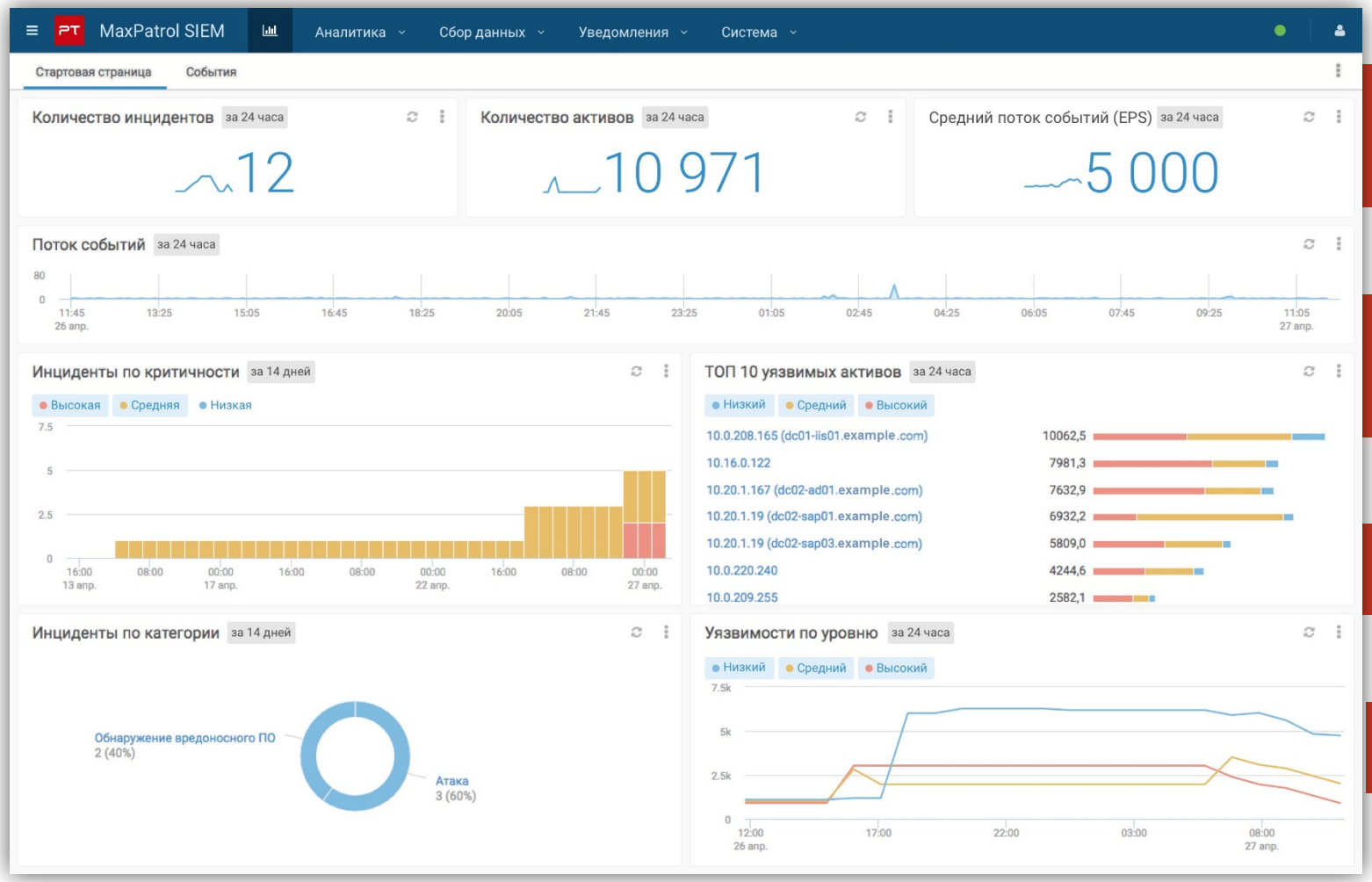
PT
KB

Информация о методах
и тактиках проведения атак,
индикаторы компрометации

Рекомендации по тонкой
настройке аудита на источниках
для точного выявления атак

MaxPatrol SIEM: визуализация и отчетность

POSITIVE TECHNOLOGIES



Настраиваемые дашборды
и пользовательские виджеты

Детализация информации
с дашбордов в один клик

Автоматическое создание отчетов

Отправка отчетов по расписанию

PT Application Firewall

Межсетевой экран уровня приложений

Web повсюду

POSITIVE TECHNOLOGIES

~3,5 млрд активных пользователей (население ~7,3)*

Охватывает практически все сферы нашей жизни

* - *по данным Международного союза электросвязи (МСЭ) от 22.07.2016*

Проблемы безопасности веб-приложений

POSITIVE TECHNOLOGIES

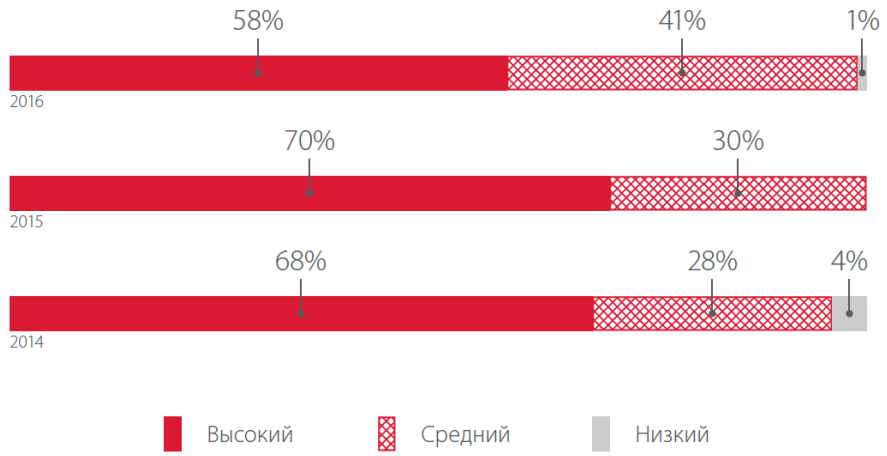
Веб-приложения стали целью злоумышленников № 1

30% 30% атак приходится на веб-приложения*

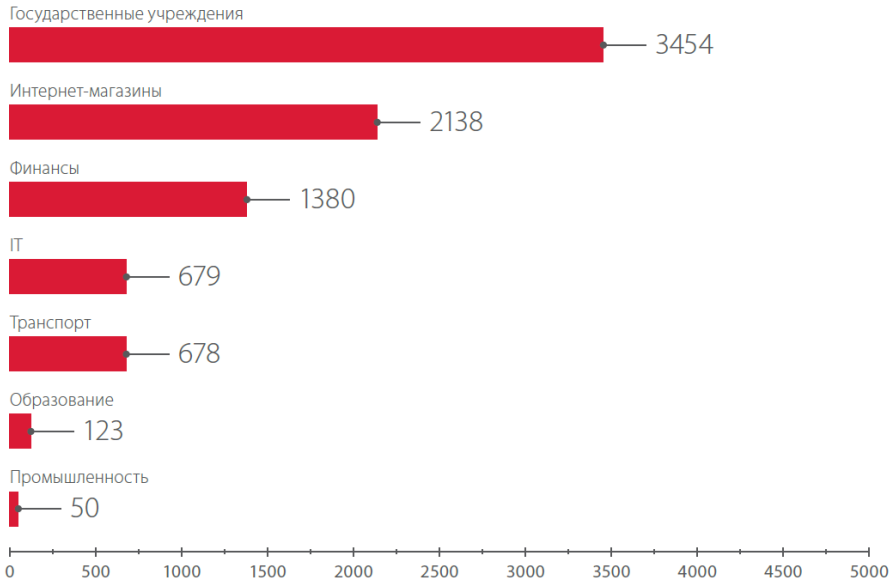
58% 58% веб-приложений содержат критически опасные уязвимости

77% В 77% случаев за периметр организации можно проникнуть через веб-уязвимости**

Также необходимо выполнять требования регуляторов (ФСТЭК, Банка России)



Доля уязвимых сайтов по степени риска уязвимостей

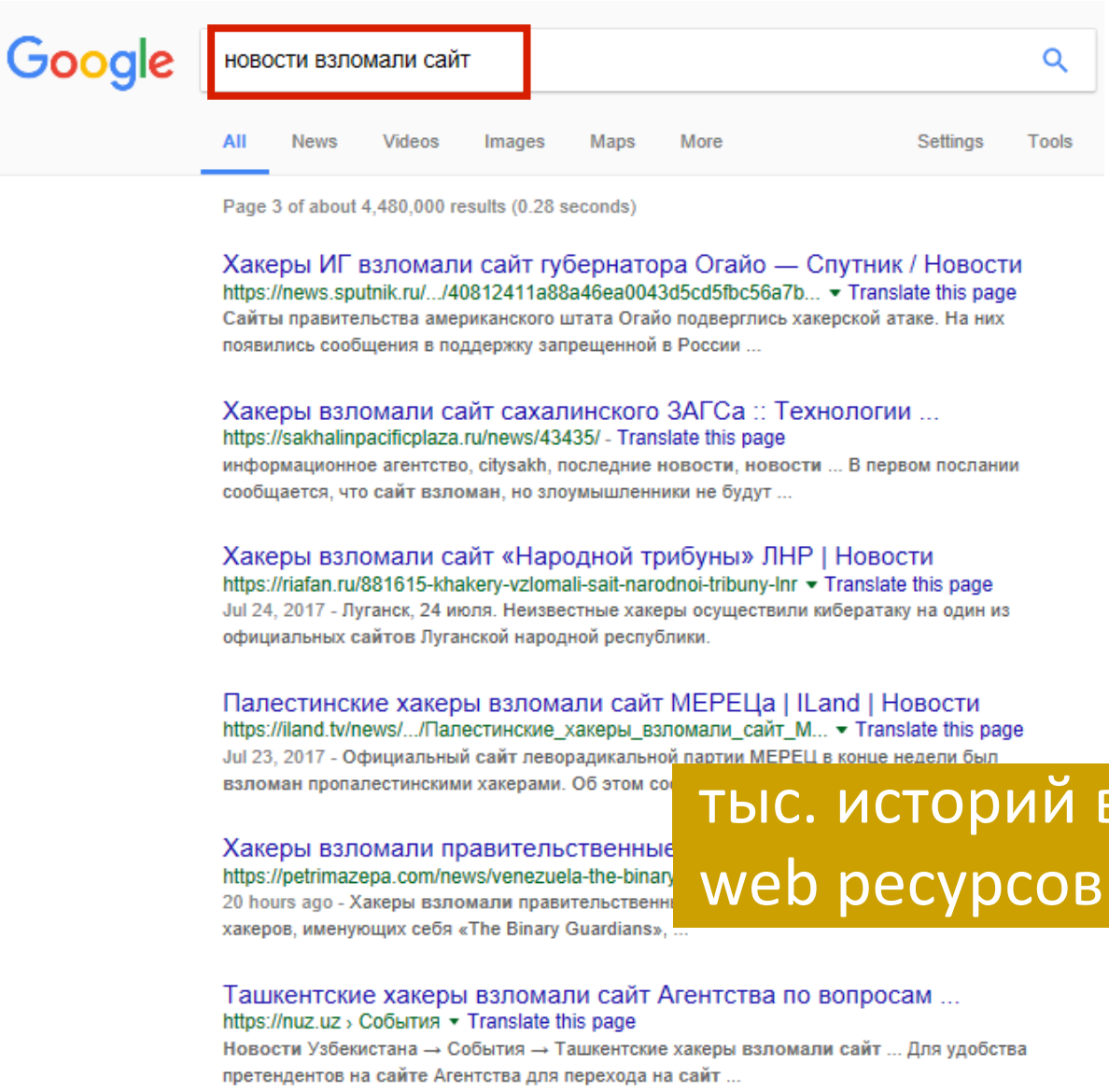


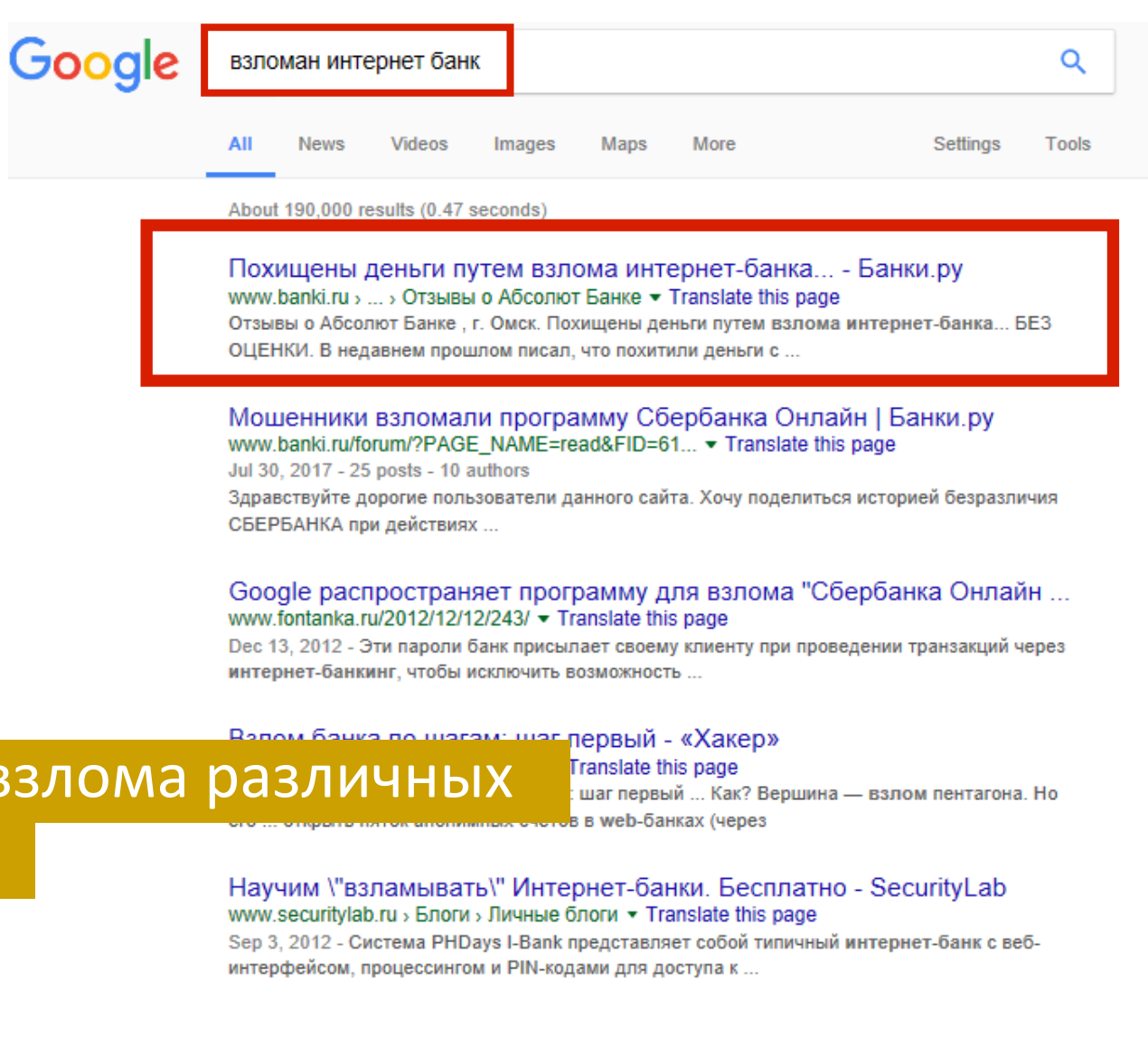
Среднее количество атак в день на одну систему

Источники:
* Verizon Data Breach report 2017
** Positive Research 2017

Подлинные истории

POSITIVE TECHNOLOGIES





тыс. историй взлома различных web ресурсов

Классические инвестиции в ИБ ≠ защита от атак на Web

POSITIVE TECHNOLOGIES

Инвестиции компаний

- Средства защиты периметра
- Средства защиты веб-приложений и их пользователей

Доли атак

- Атаки на периметр напрямую
- Атаки на периметр через веб-приложения

* - *Источник: SANS Institute, 2016*

PT Application Firewall адекватная реакция на вызовы современного Интернета

- Компания Positive Technologies является визионером магического квадранта Gartner по безопасности веб-приложений
- Positive Technologies единственная российская Компания, которая представлена в квадранте Gartner с решением данного класса

Gartner
Magic Quadrant

визионеры - компании, которые отлично понимают рынок или имеют четкое видение, как изменить правила рынка

PT Application Firewall – всесторонняя защита

POSITIVE TECHNOLOGIES

360° защита

- Web-приложения
- Пользователи
- Бизнес-логика

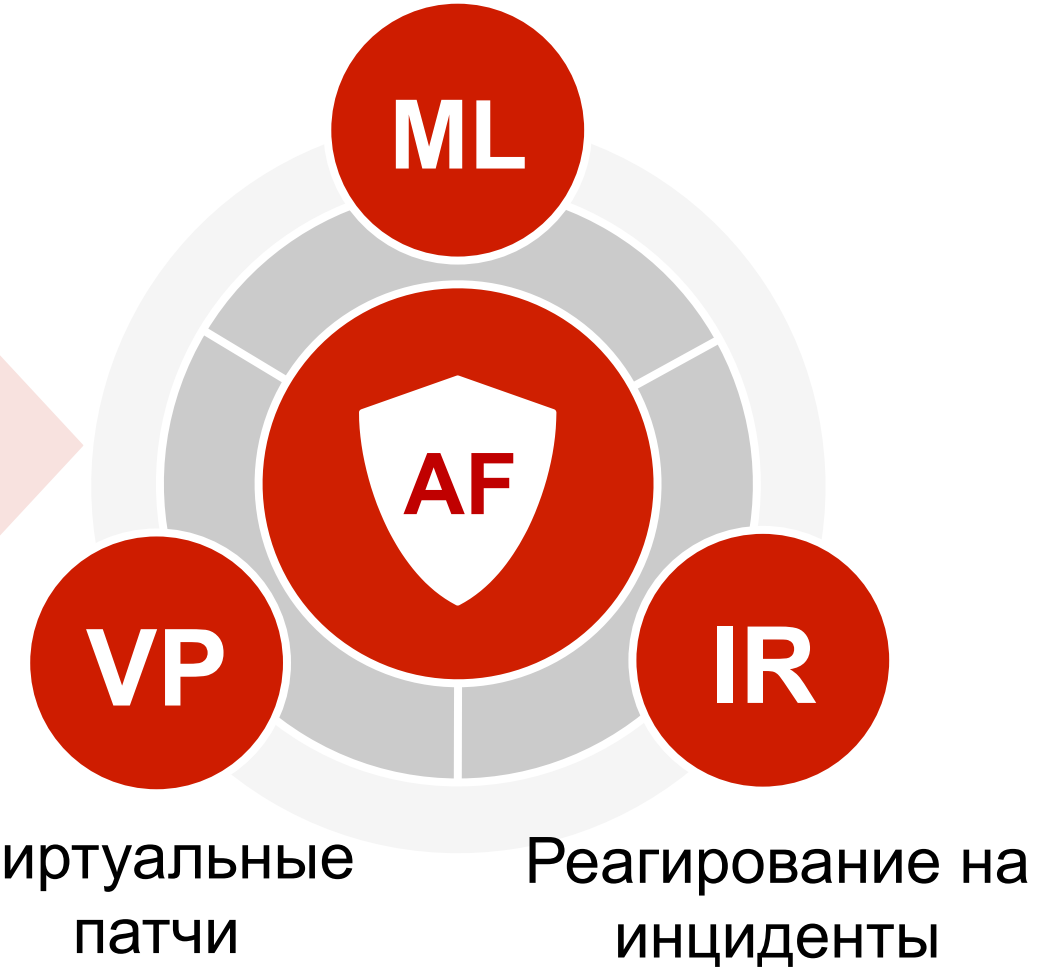
PT AF ключевые преимущества

POSITIVE TECHNOLOGIES

Позитивная модель – вероятностные алгоритмы для блокирования новых атак

Негативная модель – анализ исходных кодов для исключения возможных угроз до вывода приложения в эксплуатацию

Расследование – корреляционный движок для выявления цепочек атак



PT MultiScanner

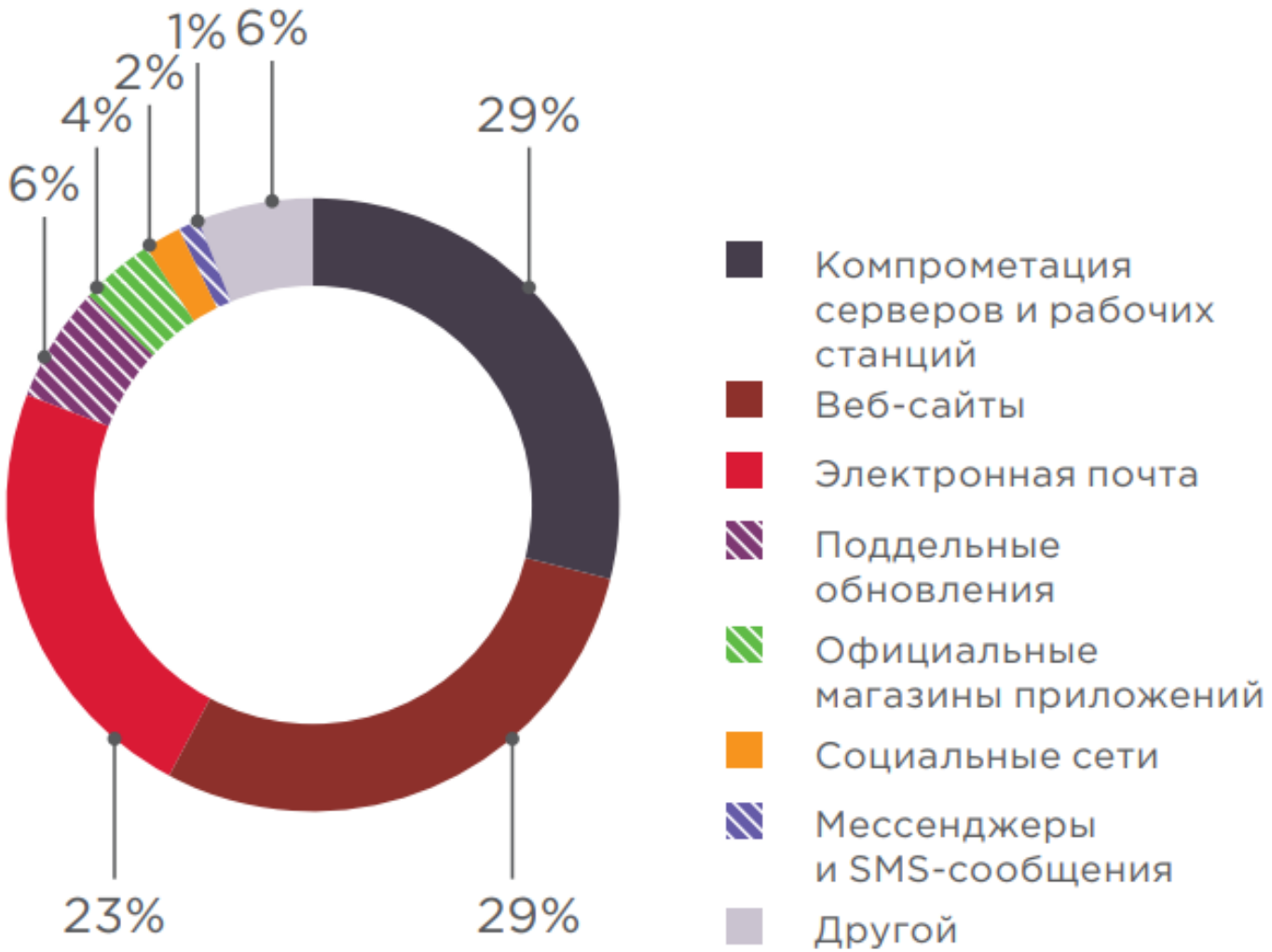
Многопоточная система выявления вредоносного контента

Использование ВПО в атаках в 2018Q2

POSITIVE TECHNOLOGIES

Шпионское ПО **26%**

ВПО для удаленного управления **22%**



PT MultiScanner – универсальная защита от вирусных атак

POSITIVE TECHNOLOGIES

Локализация угроз

Помогает локализовать и предотвратить распространение заражения по всем актуальным каналам в инфраструктуре

Мультивендорный подход

Использует для выявления вредоносного ПО несколько антивирусных движков, статический анализ и черные списки, поставляемые Positive Technologies

Единая точка мониторинга и хранения объектов

Централизованно анализирует и хранит передаваемые объекты для удобства расследования инцидентов

Ретроспективный анализ: взгляд в прошлое

POSITIVE TECHNOLOGIES

Ретроспективный анализ объектов позволяет выявлять распределенные во времени атаки и скрытое присутствие ВПО в инфраструктуре

Единое хранилище проанализированных объектов

Неограниченное по времени хранение файлов и метаданных

Автоматическое пересканирование без нагрузки на систему

Пересканирование при обновлении движков и репутационных списков

Варианты использования PT MultiScanner

POSITIVE TECHNOLOGIES

PT MultiScanner

Защита почты

Расследование инцидентов

Контроль корпоративного трафика

Внутренний сервис

Контроль файловых хранилищ

Защита веб-порталов

Контроль пользовательского веб-трафика

PT Network Attack Discovery (NAD)

Решение класса Network Forensics, предназначенное для анализа сетевого трафика и расследования инцидентов

Ф – форензика. Р – расследования.

POSITIVE TECHNOLOGIES

- Детализированный разбор более **30** наиболее распространенных протоколов
- Хранение **всего** сырого трафика с разделением на отдельные сессии
- **3000+** собственных сигнатур, качество которых признано мировыми лидерами ET, Cisco Talos
- **Сквозной поиск** по множеству полей протоколов (более 1000)
- Глубокая интеграция с экосистемой **PT: PT MultiScanner, MaxPatrol SIEM**

Изображение: adolfrodriguez.com/home-2/investigation-wall/

Детализированный разбор трафика

POSITIVE TECHNOLOGIES

- Географическая принадлежность IP-адресов, участвующих в сетевом взаимодействии
- Извлеченные файлы и данные, передаваемые по протоколам прикладного уровня
- Определение имен, типов передаваемых файлов и их контрольных сумм
- Сбор информации о баннерах сетевых приложений
- Постоянная индексация в режиме реального времени всего захватываемого сетевого трафика с сохранением в БД полученной информации:
  - время (начало, конец сессии);
  - IP-адреса узлов;
  - протокол транспортного уровня;
  - номера портов;
  - протокол прикладного уровня;
  - объем переданных данных;
  - доменные имена узлов;
  - разобранные поля протоколов прикладного уровня.

Простота восприятия данных

POSITIVE TECHNOLOGIES

Общие сведения

Протоколы	http, tcp
Начало	27 июня 2018, 12:13:00
Конец	27 июня 2018, 12:13:02
Длительность	0 секунд
Отправлено	3 кБ, 49 пакетов
Получено	746 кБ, 505 пакетов
Отправитель	154.179.83.221:34745 [AS8452 TE-AS] (EG) Египет 00:0C:29:92:67:E1
Получатель	179.241.18.181:80 [AS22085 Claro S/A] (BR) Бразилия 00:0C:29:79:FD:9E
Хранилище	Challenge
PCAP-файлы	/opt/ptsecurity/data/persistent/48/thread-0/2018-02-19_17/log_2018-02-19.0.1519...

Атаки

[PT OPEN] Metasploit MS17-010 ETERNALCHAMPION Successful kernel data leak (CVE-2017-0146)
Attempted Administrator Privilege Gain

[PT OPEN] Metasploit MS17-010 ETERNALROMANCE exploitation (CVE-2017-0143)
Attempted Administrator Privilege Gain

[PT OPEN] Metasploit MS17-010 ETERNALCHAMPION Successful kernel data leak (CVE-2017-0146)
Attempted Administrator Privilege Gain

Еще 1 атака

Файлы

EXE ddd.exe 718.34 кБ
/

Учетные записи

administrator 123456789

HTTP

19.02.18 20:32:06	GET	/ddd.exe 154.179.83.221:34745	0 Б	OK 200	application/x-msdos-program	718.34 кБ UNKNOWN	

Простота восприятия данных

POSITIVE TECHNOLOGIES

Общие сведения

Протоколы	http, tcp
Начало	27 июня 2018, 12:13:00
Конец	27 июня 2018, 12:13:02
Длительность	0 секунд
Отправлено	3 кБ, 49 пакетов
Получено	746 кБ, 505 пакетов
Отправитель	154.179.83.221:34745 [AS8452 TE-AS] (EG) Египет 00:0C:29:92:67:E1
Получатель	179.241.18.181:80 [AS22085 Claro S/A] (BR) Бразилия 00:0C:29:79:FD:9E
Хранилище	Challenge
PCAP-файлы	/opt/ptsecurity/data/persistent/48/thread-0/2018-02-19_17/log_2018-02-19.0.1519...

Атаки

[PT OPEN] Metasploit MS17-010 ETERNALCHAMPION Successful kernel data leak (CVE-2017-0146)
Attempted Administrator Privilege Gain

[PT OPEN] Metasploit MS17-010 ETERNALROMANCE exploitation (CVE-2017-0143)
Attempted Administrator Privilege Gain

[PT OPEN] Metasploit MS17-010 ETERNALCHAMPION Successful kernel data leak (CVE-2017-0146)
Attempted Administrator Privilege Gain

Еще 1 атака

Файлы

EXE ddd.exe 718.34 кБ
/

Учетные записи

administrator 123456789

HTTP

19.02.18 20:32:06	GET	/ddd.exe 154.179.83.221:34745	0 Б	OK 200	application/x-msdos-program	718.34 кБ UNKNOWN

Простота восприятия данных

POSITIVE TECHNOLOGIES

Общие сведения

Протоколы	http, tcp
Начало	27 июня 2018, 12:13:00
Конец	27 июня 2018, 12:13:02
Длительность	0 секунд
Отправлено	3 кБ, 49 пакетов
Получено	746 кБ, 505 пакетов
Отправитель	154.179.83.221:34745 [AS8452 TE-AS] (EG) Египет 00:0C:29:92:67:E1
Получатель	179.241.18.181:80 [AS22085 Claro S/A] (BR) Бразилия 00:0C:29:79:FD:9E
Хранилище	Challenge
PCAP-файлы	/opt/ptsecurity/data/persistent/48/thread-0/2018-02-19_17/log_2018-02-19.0.1519...

Атаки

[PT OPEN] Metasploit MS17-010 ETERNALCHAMPION Successful kernel data leak (CVE-2017-0146)
Attempted Administrator Privilege Gain

[PT OPEN] Metasploit MS17-010 ETERNALROMANCE exploitation (CVE-2017-0143)
Attempted Administrator Privilege Gain

[PT OPEN] Metasploit MS17-010 ETERNALCHAMPION Successful kernel data leak (CVE-2017-0146)
Attempted Administrator Privilege Gain

Еще 1 атака

Файлы

EXE ddd.exe 718.34 кБ
/

Учетные записи

administrator 123456789

HTTP

19.02.18 20:32:06	GET	/ddd.exe 154.179.83.221:34745	0 Б	OK 200	application/x-msdos-program	718.34 кБ UNKNOWN	

Простота восприятия данных

POSITIVE TECHNOLOGIES

Общие сведения

Протоколы	http, tcp
Начало	27 июня 2018, 12:13:00
Конец	27 июня 2018, 12:13:02
Длительность	0 секунд
Отправлено	3 кБ, 49 пакетов
Получено	746 кБ, 505 пакетов
Отправитель	154.179.83.221:34745 [AS8452 TE-AS] (EG) Египет 00:0C:29:92:67:E1
Получатель	179.241.18.181:80 [AS22085 Claro S/A] (BR) Бразилия 00:0C:29:79:FD:9E
Хранилище	Challenge
PCAP-файлы	/opt/ptsecurity/data/persistent/48/thread-0/2018-02-19_17/log_2018-02-19.0.1519...

Атаки

[PT OPEN] Metasploit MS17-010 ETERNALCHAMPION Successful kernel data leak (CVE-2017-0146)
Attempted Administrator Privilege Gain

[PT OPEN] Metasploit MS17-010 ETERNALROMANCE exploitation (CVE-2017-0143)
Attempted Administrator Privilege Gain

[PT OPEN] Metasploit MS17-010 ETERNALCHAMPION Successful kernel data leak (CVE-2017-0146)
Attempted Administrator Privilege Gain

Еще 1 атака

Файлы

EXE ddd.exe 718.34 кБ
/

Учетные записи

administrator	123456789

Все файлы скачиваемые

HTTP

19.02.18 20:32:06	GET	/ddd.exe 154.179.83.221:34745	0 Б	OK 200	application/x-msdos-program	718.34 кБ UNKNOWN

Простота восприятия данных

POSITIVE TECHNOLOGIES

Общие сведения

Протоколы	http, tcp
Начало	27 июня 2018, 12:13:00
Конец	27 июня 2018, 12:13:02
Длительность	0 секунд
Отправлено	3 кБ, 49 пакетов
Получено	746 кБ, 505 пакетов
Отправитель	154.179.83.221:34745 [AS8452 TE-AS] (EG) Египет 00:0C:29:92:67:E1
Получатель	179.241.18.181:80 [AS22085 Claro S/A] (BR) Бразилия 00:0C:29:79:FD:9E
Хранилище	Challenge
PCAP-файлы	/opt/ptsecurity/data/persistent/48/thread-0/2018-02-19_17/log_2018-02-19.0.1519...

Атаки

[PT OPEN] Metasploit MS17-010 ETERNALCHAMPION Successful kernel data leak (CVE-2017-0146)
Attempted Administrator Privilege Gain

[PT OPEN] Metasploit MS17-010 ETERNALROMANCE exploitation (CVE-2017-0143)
Attempted Administrator Privilege Gain

[PT OPEN] Metasploit MS17-010 ETERNALCHAMPION Successful kernel data leak (CVE-2017-0146)
Attempted Administrator Privilege Gain

Еще 1 атака

Файлы

EXE ddd.exe 718.34 кБ
/

Учетные записи

administrator 123456789

Все файлы скачиваемые

HTTP

19.02.18 20:32:06	GET	/ddd.exe 154.179.83.221:34745	0 Б	OK 200	application/x-msdos-program	718.34 кБ UNKNOWN

Логинов Роман
Менеджер по продвижению продуктов
rloginov@ptsecurity.com
+7 903 737 4122

Спасибо за внимание!

POSITIVE TECHNOLOGIES

ptsecurity.ru