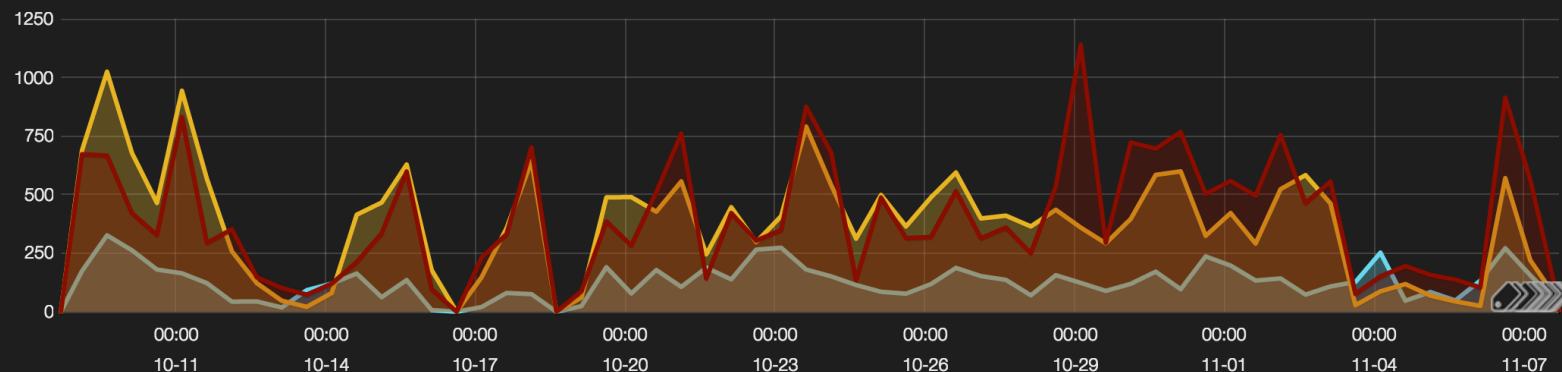


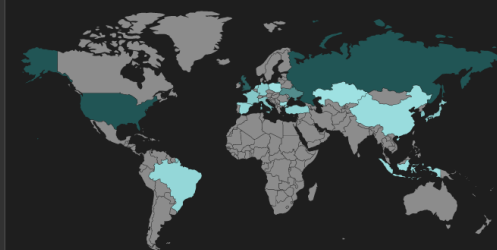
FILTERING ▾

ATTACK DYNAMICS

🔍 Уменьшить | ● EVENT_SEVERITY:low (7696) ● EVENT_SEVERITY:medium (22999) ● EVENT_SEVERITY:high (24097) count per 12h | (54792 hits)



COUNTRIES



ALERTS

0 до 7 из 298 доступных записей →

ALERT_SEVERITY ▾

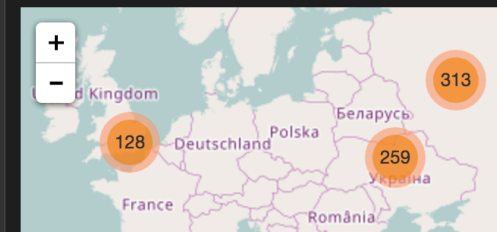
STATUS ▾

ALERT_NAME ▾

TIMESTAMP ▾

ongoing	Confirmed vulnerability	2016-11-07 16:02:11
finished	Automated vulnerability scanning	2016-11-07 14:52:38
finished	Web spamming	2016-11-07 14:41:40

CITIES



WAF, который смог

Positive Technologies Application Firewall

«**Positive Technologies** is rated as a Visionary because of its execution on a security-driven roadmap. Organizations that are looking for high security first should consider adding Positive Technologies to their shortlists, but verify the level of local expertise on and support for the technology.»

from Gartner Magic Quadrant



PT Application Firewall

POSITIVE TECHNOLOGIES

Машинное обучение

- Доступ по модели белых списков
- Защита от неизвестных уязвимостей
- Определение скрытых попыток взлома

Минимум False Positive

- Встроенный сканер для поиска уязвимостей
- Инструменты для формирования корреляций
- Визард для исключений прямо на дэшборде



Виртуальные патчи

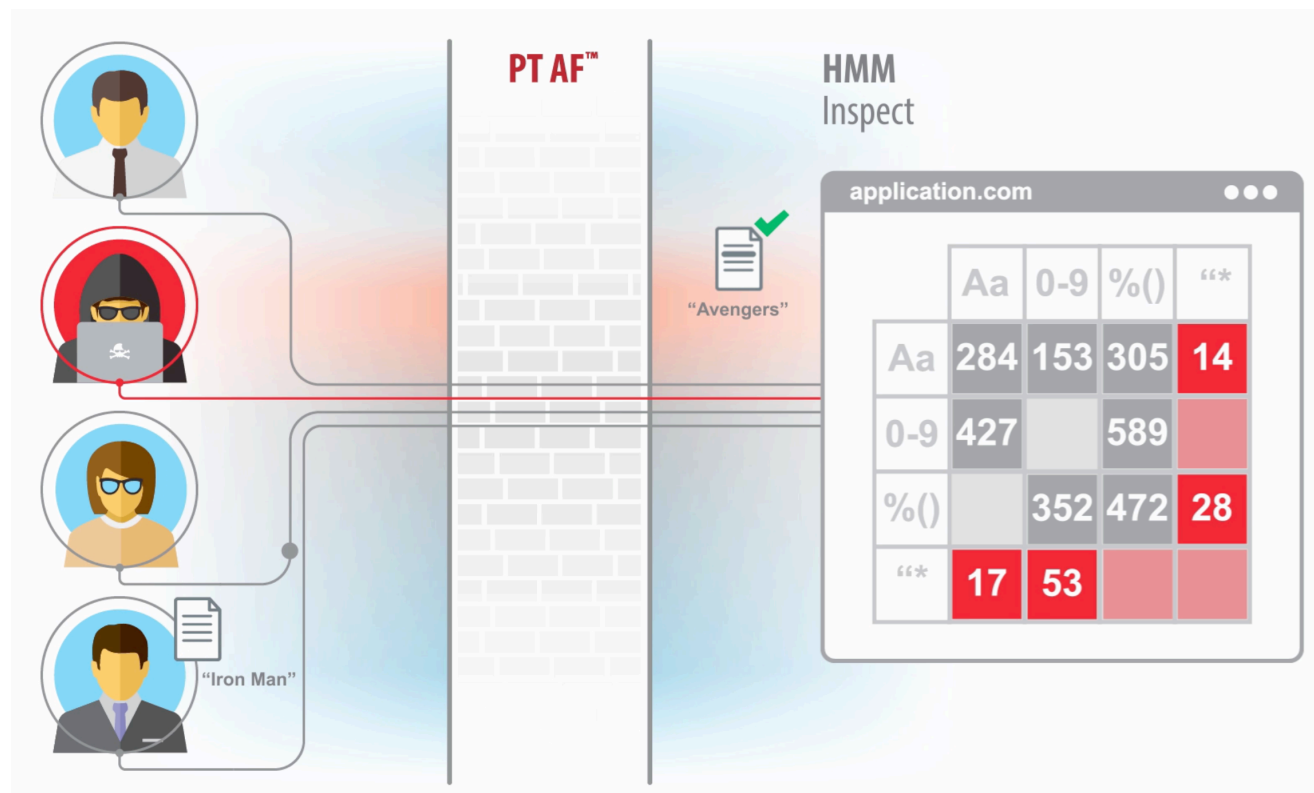
- Гарантированная защита от уязвимостей
- Идеально для уже работающих сайтов
- Наиболее правильный подход к ИБ

Поведенческий анализ и поиск аномалий

- Определение ботов
- Защита от DDoS атак 7-го уровня
- Stress-based алгоритм

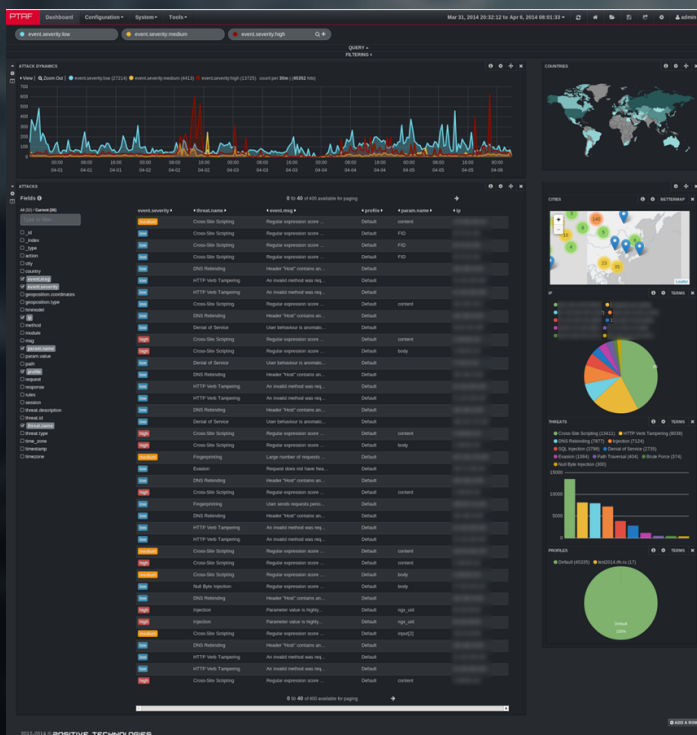
Машинное обучение

POSITIVE TECHNOLOGIES



- Группы символов, а не отдельные знаки
- Отдельная модель для каждого атрибута запроса (параметр, заголовок, cookie)
- Итеративное обучение
- Обнаружение и фильтрация выбросов
- Отслеживание ошибок и автоматическое переобучение
- Возможность ручного предобучения

Минимум False Positive

POSITIVE TECHNOLOGIES

Attacks (12564)

Attack chains (11)

chain.stat ▶	◀ chain.dynamic ▶	◀ lastthreat.name ▶	◀ last.timestamp ▼	◀ ip ▶
		SQL Injection	2014-04-12T01:29:13.992	192.168.1.100
		SQL Injection	2014-04-12T00:17:17.638	192.168.1.100
		SQL Injection	2014-04-12T00:17:17.567	192.168.1.100
		SQL Injection	2014-04-11T22:49:53.000	192.168.1.100
		SQL Injection	2014-04-11T22:48:59.000	192.168.1.100
		Path Traversal	2014-04-11T22:47:07.521	192.168.1.100
		Path Traversal	2014-04-11T22:46:50.000	192.168.1.100
		Cross-Site Scripting	2014-04-11T22:38:32.000	192.168.1.100
		Cross-Site Scripting	2014-04-11T22:21:25.320	192.168.1.100
		Cross-Site Scripting	2014-04-11T21:57:14.450	192.168.1.100
		SQL Injection	2014-04-11T21:57:10.715	192.168.1.100

COUNTRIES

IP

Виртуальные патчи

POSITIVE TECHNOLOGIES

PTTF Dashboard Configuration System Tools admin

VIRTUAL PATCHING

Step 1. Create new virtual patch
You can create new virtual patch manually or import Application Inspector report

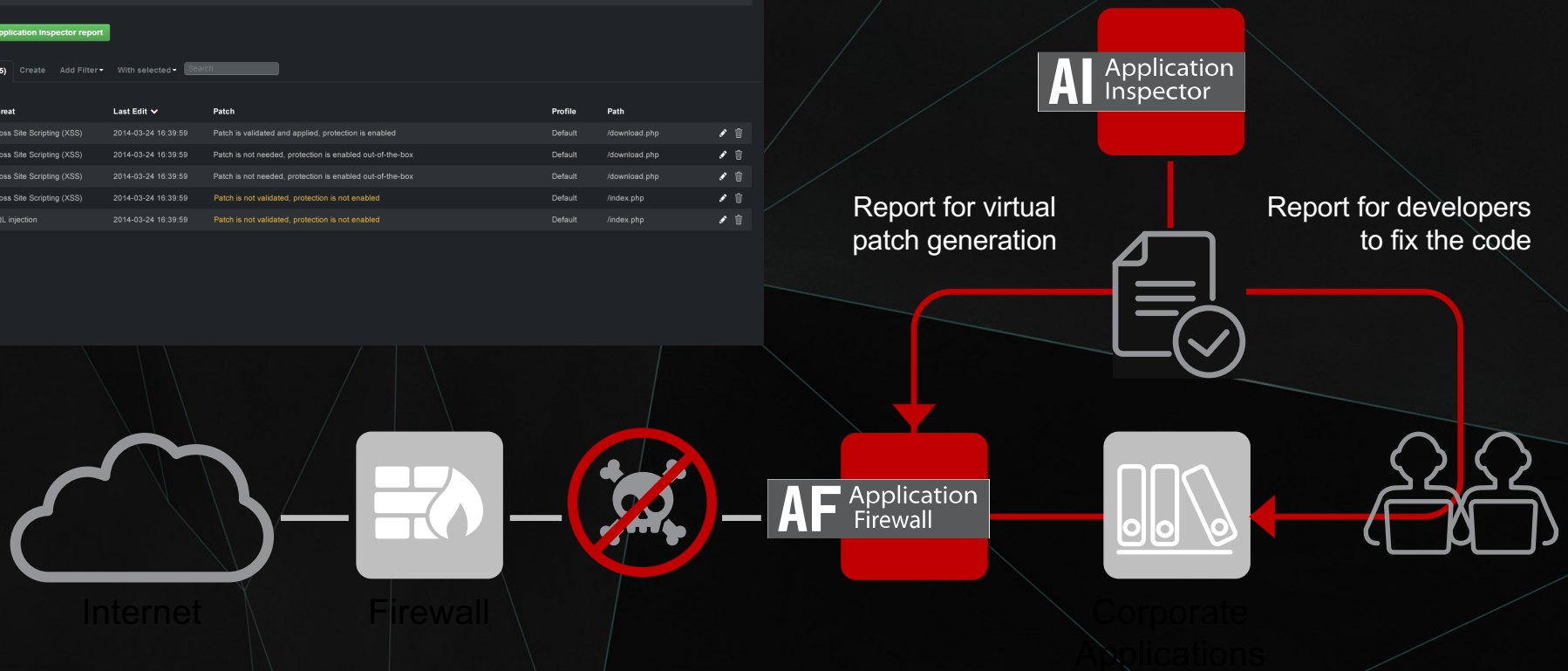
Step 2. Validate virtual patch
Application Firewall will validate virtual patch if it fixes vulnerability properly, you can also review it manually

Step 3. Apply virtual patch
After virtual patch is validated you can apply it to take immediate effect

Import Application Inspector report

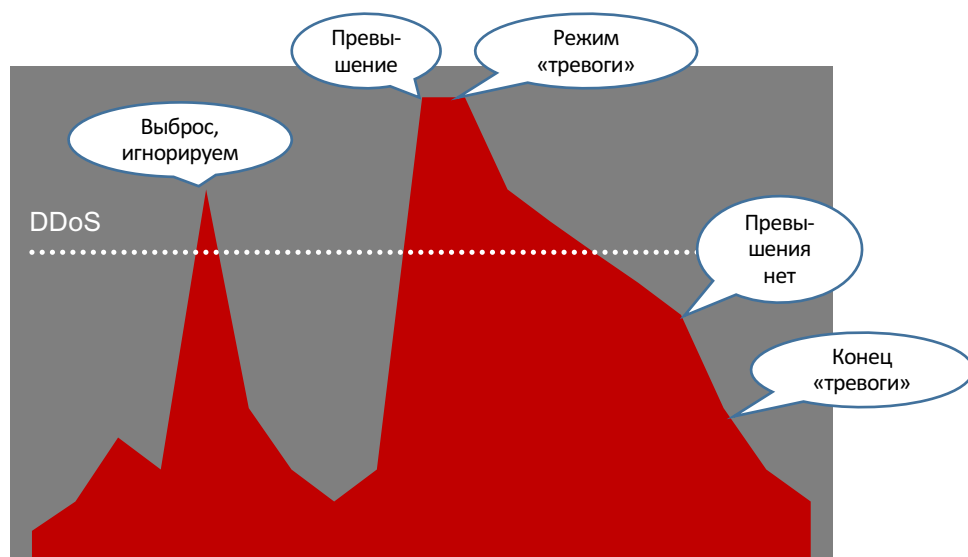
Threats (5) Create Add Filter With selected Search

Threat	Last Edit	Patch	Profile	Path
Cross Site Scripting (XSS)	2014-03-24 16:39:59	Patch is validated and applied, protection is enabled	Default	/download.php
Cross Site Scripting (XSS)	2014-03-24 16:39:59	Patch is not needed, protection is enabled out-of-the-box	Default	/download.php
Cross Site Scripting (XSS)	2014-03-24 16:39:59	Patch is not needed, protection is enabled out-of-the-box	Default	/download.php
Cross Site Scripting (XSS)	2014-03-24 16:39:59	Patch is not validated, protection is not enabled	Default	/index.php
SQL Injection	2014-03-24 16:39:59	Patch is not validated, protection is not enabled	Default	/index.php



Поиск аномалий и защита от DDoS

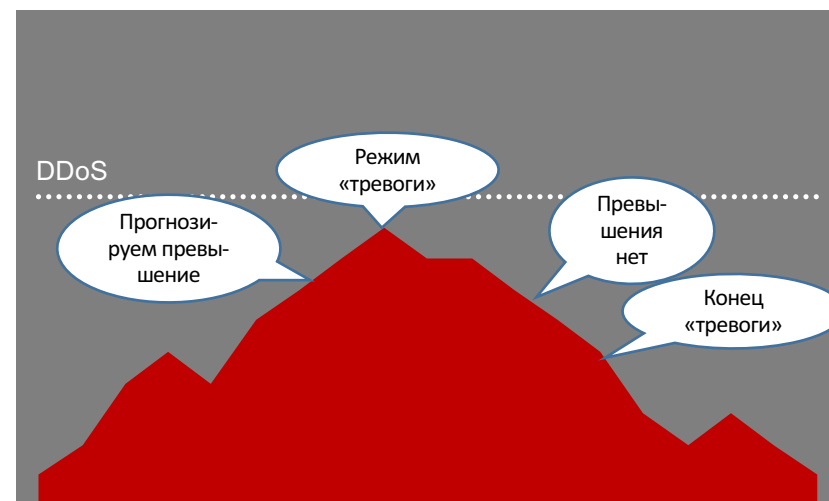
POSITIVE TECHNOLOGIES



Явное обнаружение

Thresholds

- Requests per second
- Application response time
- Application error rate
- # of new users



Прогнозирование

Mitigations

- Drop request
- Block w/ iptables
- Send to Check Point
- Send to Arbor
- Custom action (script exec)

