ОСНОВНЫЕ ВОЗМОЖНОСТИ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ HP TIPPINGPOINT

Наумов Илья
Старший специалист отдела технических решений
АО «ДиалогНаука»

ДиалогНаука

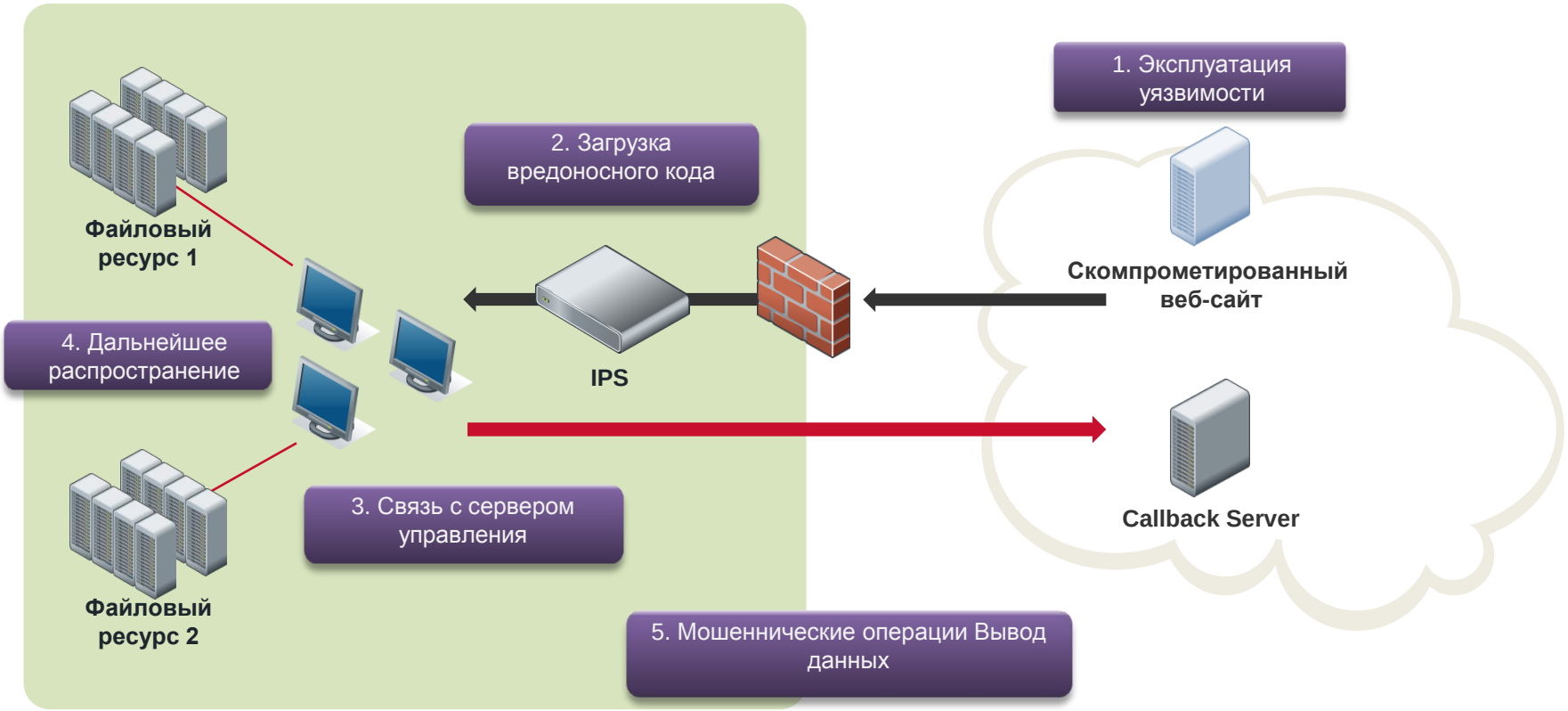
Актуальные угрозы ИБ

ДиалогНаука

Типичная атака

Детектирование эксплойтов очень важно!

Все последующие этапы могут быть скрыты



Линейка HP TippingPoint

ДиалогНаука

HP TippingPoint

IPS нового поколения

- Глубокий анализ сетевого трафика на известные уязвимости

Digital Vaccine Labs

- Ведущая лаборатория по анализу угроз
- Анализ актуальных угроз в день из обнаружения

Межсетевой экран нового поколения

- Корпоративный межсетевой экран и IPS нового поколения
- Подробный контроль приложений

Система управления безопасностью

- Централизованное управление FW и IPS
- Единая консоль для управления и оборудованием и политиками

Advanced Threat Appliance (ATA)

- Поддерживает проверку более 100 протоколов
- Защищает от потенциальных атак «нулевого дня» и «горизонтального» распространения

HP TippinPoint IPS

Платформа IPS

Разработана для будущих требований и сервисов

Полезность

- Линейная надежность
- Линейная производительность
- Точность фильтров

Безопасность

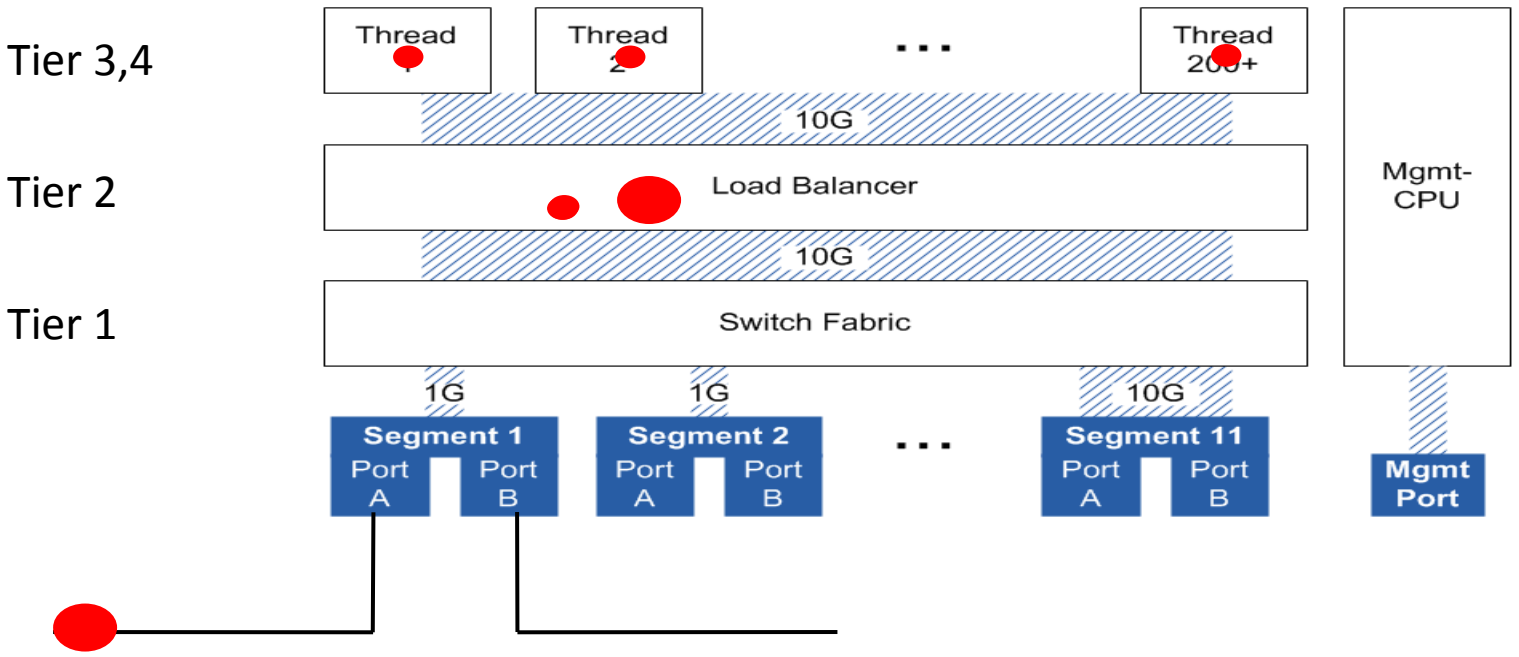
- Лидирующая исследовательская группа
- Быстрая реакция на угрозы
- Широчайший охват

Стоимость

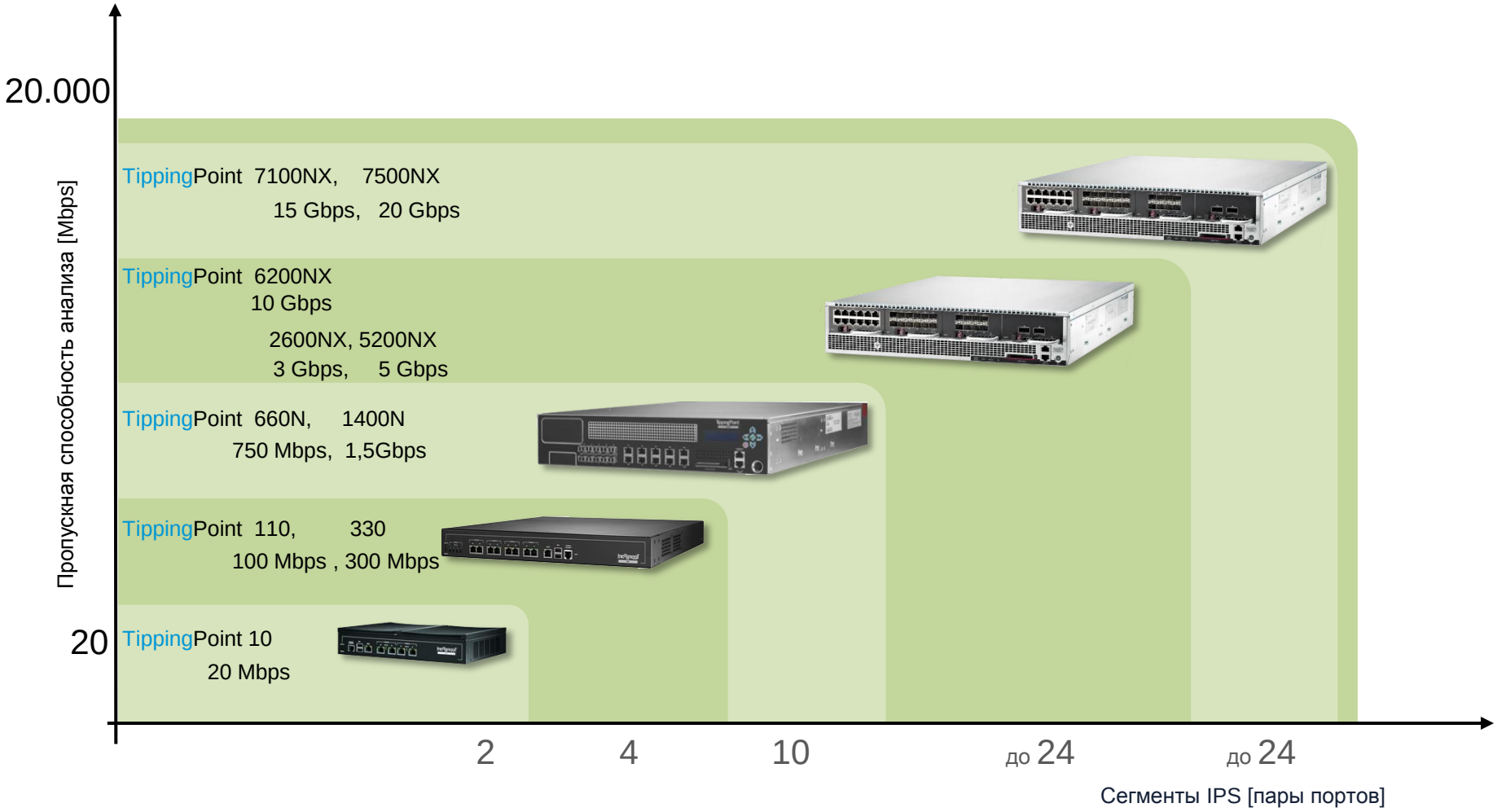
- Легкая в развертывании
- Автоматизированное блокирование угроз
- Легкая в управлении

HP TippinPoint IPS

TSE ядро предотвращения угроз



Модельный ряд



Модельный ряд

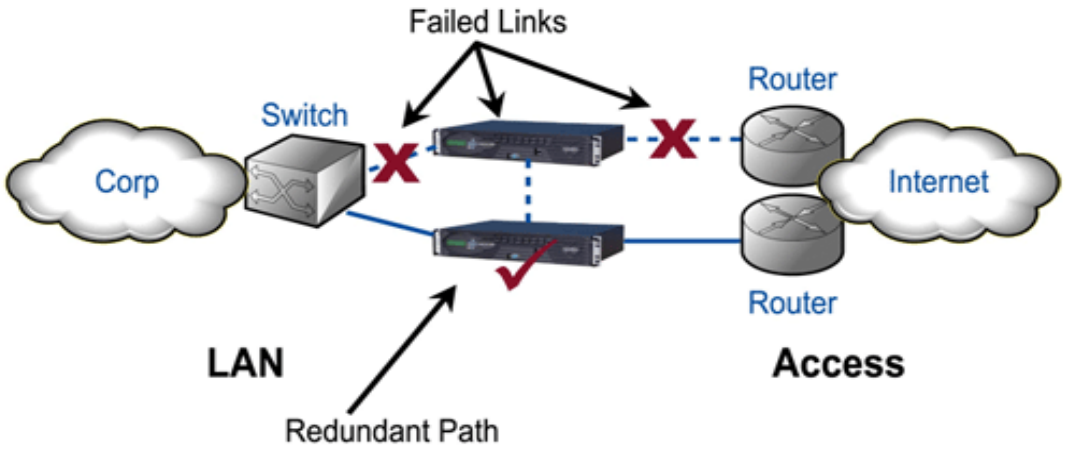
NGIPS Appliance	Inspection Thrgp. [Mbps]	Inline IPS Segments	Ports	Network Thrgp. [Mbps]	Connections per Second	Concurrent Sessions
10	20	2		**20**	**3.600**	1.000.000
110	100	4		**100**	**9.700**	1.000.000
330	300	4		**300**	**18.500**	1.000.000
660 N	750	10		**750**	**115.000**	6.500.000
1400 N	1.500	10		**1.500**	**115.000**	6.500.000
2600 NX	3.000	≤24		**40.000**	**300.000**	30.000.000
5200 NX	5.000	≤24		**40.000**	**300.000**	30.000.000
6200 NX	10.000	≤24		**40.000**	**450.000**	60.000.000
7100 NX	15.000	≤24		**100.000**	**450.000**	60.000.000
7500 NX	20.000	≤24		**100.000**	**450.000**	60.000.000

1Gbps Ethernet Copper
1Gbps Ethernet Fiber
10Gbps Ethernet Fiber
40Gbps Ethernet Fiber

Отказоустойчивость

Методы обеспечения отказоустойчивости

- Разделение Control-Plane и Data-Plane
- Дублирование блоков питания (только серии N и NX)
- ZPHA (zero-power high ability)
- Intrinsic HA (L2 failback)
- Transparent HA
- Архитектурные методы



Система управления безопасностью (SMS)

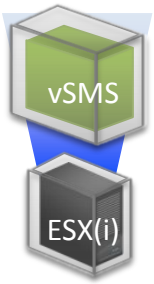
HP Security Management System H3 Appliance

HP DL360
1U
2x600Gb диски (RAID1)

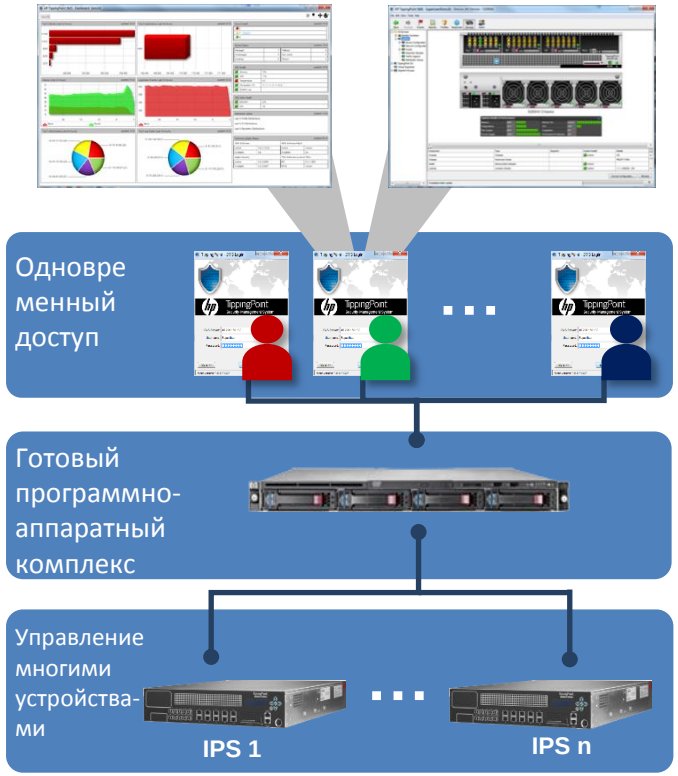
HP Security Management System H3 XL Appliance

HP DL380
2U
6x600Gb диски (RAID 1+0)

vSMS

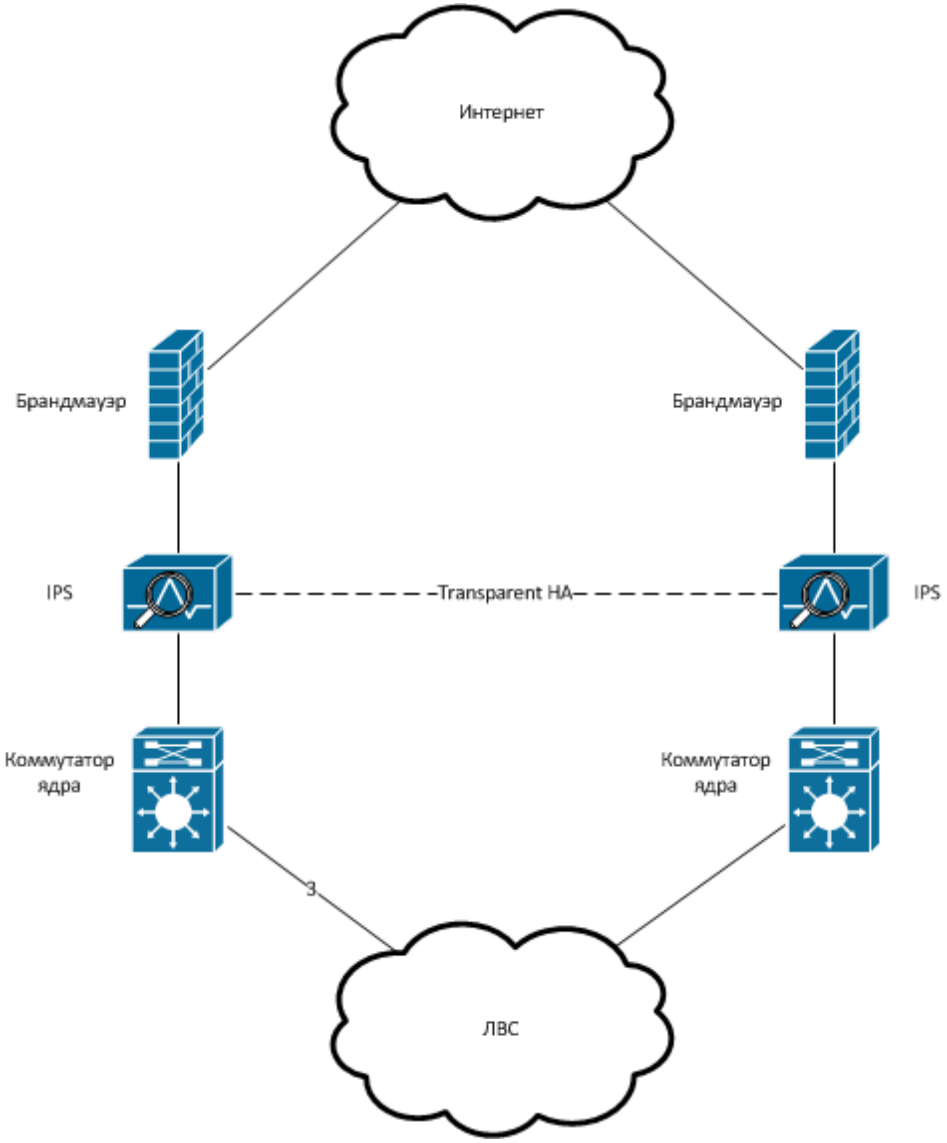


VMware ESX/ESXi v4.0 или новее
Требует vCenter
Требования:
- 300GB на диске
- 2 virtual CPU
- 6GB available memory
- 2 virtual network adapters



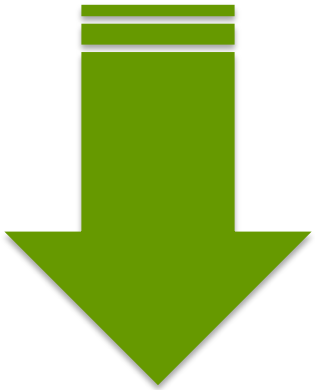
Варианты реализации

- Зеркалирование трафика
- Установка «в разрыв»
- Установка «на палке»
- Комбинированный подход
- Обеспечение отказоустойчивости на двух каналах



Управление сегментами и политиками

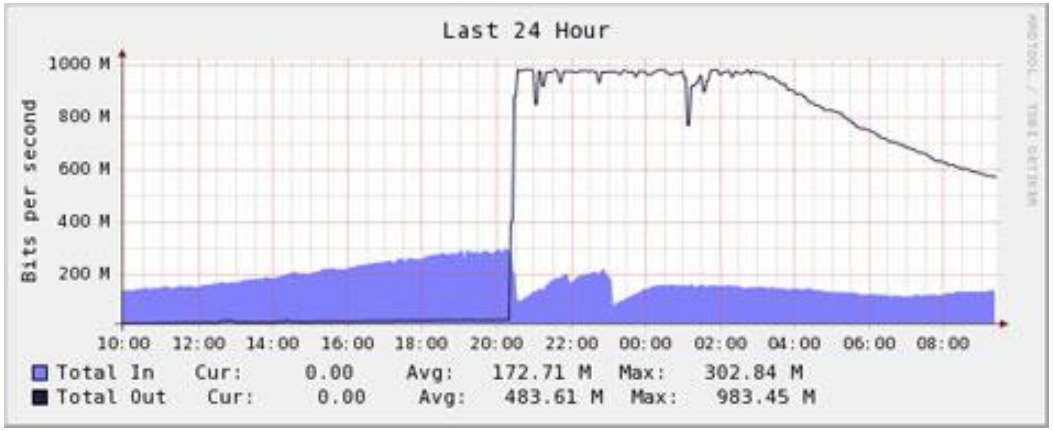
- Несколько аппаратных сегментов разных устройств могут объединяться в виртуальные сегменты
- Виртуальные сегменты можно выделять на уровне VLAN id и/или подсети
- Для каждого сегмента можно устанавливать свою уникальную политику безопасности



- Для любой сети\сервиса в организации можно задать уникальную политику в рамках всей системы централизованного управления.

Политика безопасности

Анти DoS\DDoS



Методы обеспечения защиты от DoS\DDoS

- SYN Proxy
- Quarantine
- RepDV
- IPS Filters
- DV-Toolkit
- Интеграция с другим оборудованием\представителями услуг связи

Интеграция

Протоколы:

- Syslog
- Email\SNMP-trap
- SNMP
- Web-API

Назначения:

- Корреляция событий ИБ (SIEM, например HP ArcSight)
- Мониторинг оборудования (в реальном времени и на уровне событий)
- Взаимодействие с другими системами в режиме управления (ведущий и ведомый)
- Все, что Вы еще сможете придумать

HP TippingPoing ATA

ДиалогНаука

Обзор

- Настройка «песочниц» под заказчика, не требующая дополнительных плат
- Устройства производительностью от 250 Мбит до 4 Гбит
- Интеграция с остальной инфраструктурой HP Security

Модель	Количество «песочниц»	Производитель-ность
ATA 250	1	250 Mbps
ATA 500	4	500 Mbps
ATA 1000	4	1 Gbps
ATA 4000	20	4 Gbps
ATA Mail 6000	24	400,000 emails/day

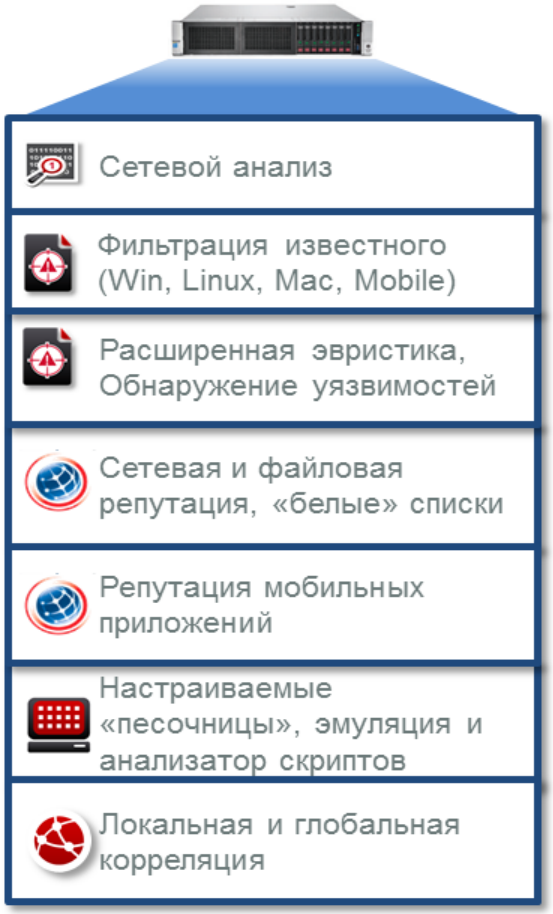
TippingPoint ATA

Обнаружение

Вредоносное содержимое
Эксплоиты в документах
Встраиваемые загрузчики (Drive-by)
Эксплоиты 0-дня
ВПО (известное и неизвестное)

Подозрительные взаимодействия
C&C обращения
Кража данных
Черви
Backdoor -активность…

Признаки атаки
Распространение и загрузка
Сканирования и подбор паролей
Вывод данных…



100+ протоколов на любом порту!

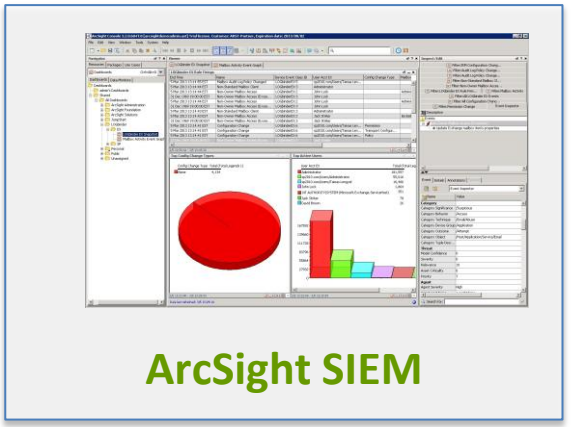
- Поддерживает анализ не только «вертикальных» потоков трафика, но так же и «горизонтальных».
- Адаптация к уникальной инфраструктуре заказчика
- Объединяет технологии Trend Micro и облачные сервисы HP TippingPoint

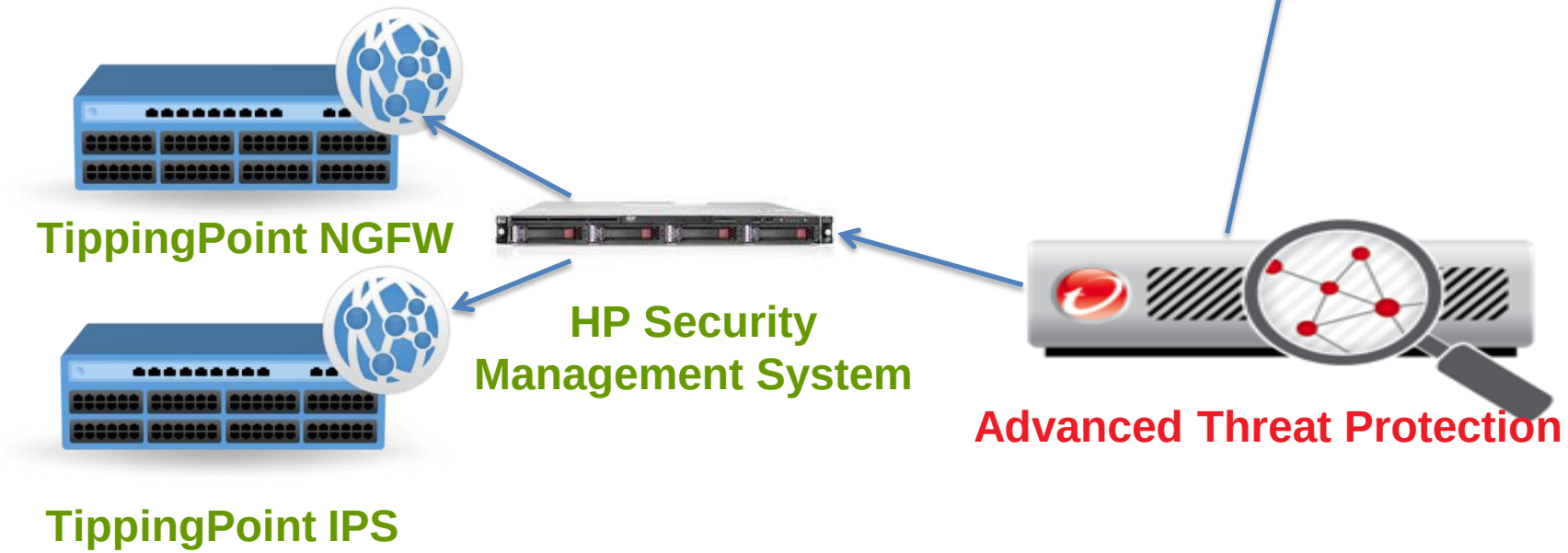
Интеграция

Информация об обнаруженных АТА ВПО может быть распространена:

- **TippingPoint IPS**
- **TippingPoint NGFW**
- **ArcSight SIEM**

Для блокировки возможных атах, корреляции в SIEM или изоляции зараженных АРМ

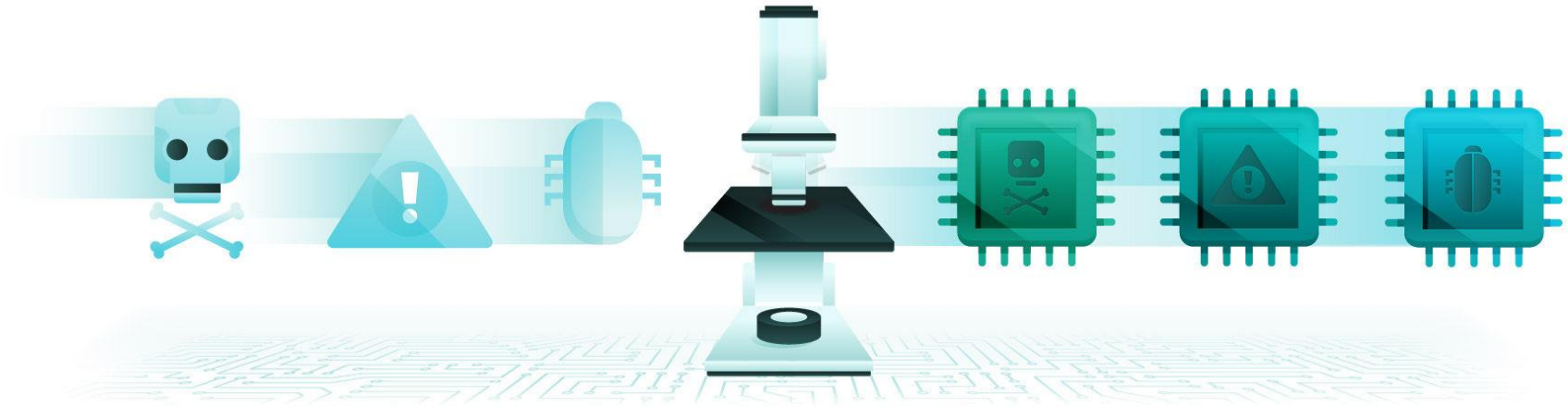




Лаборатория DVLabs

ДиалогНаука

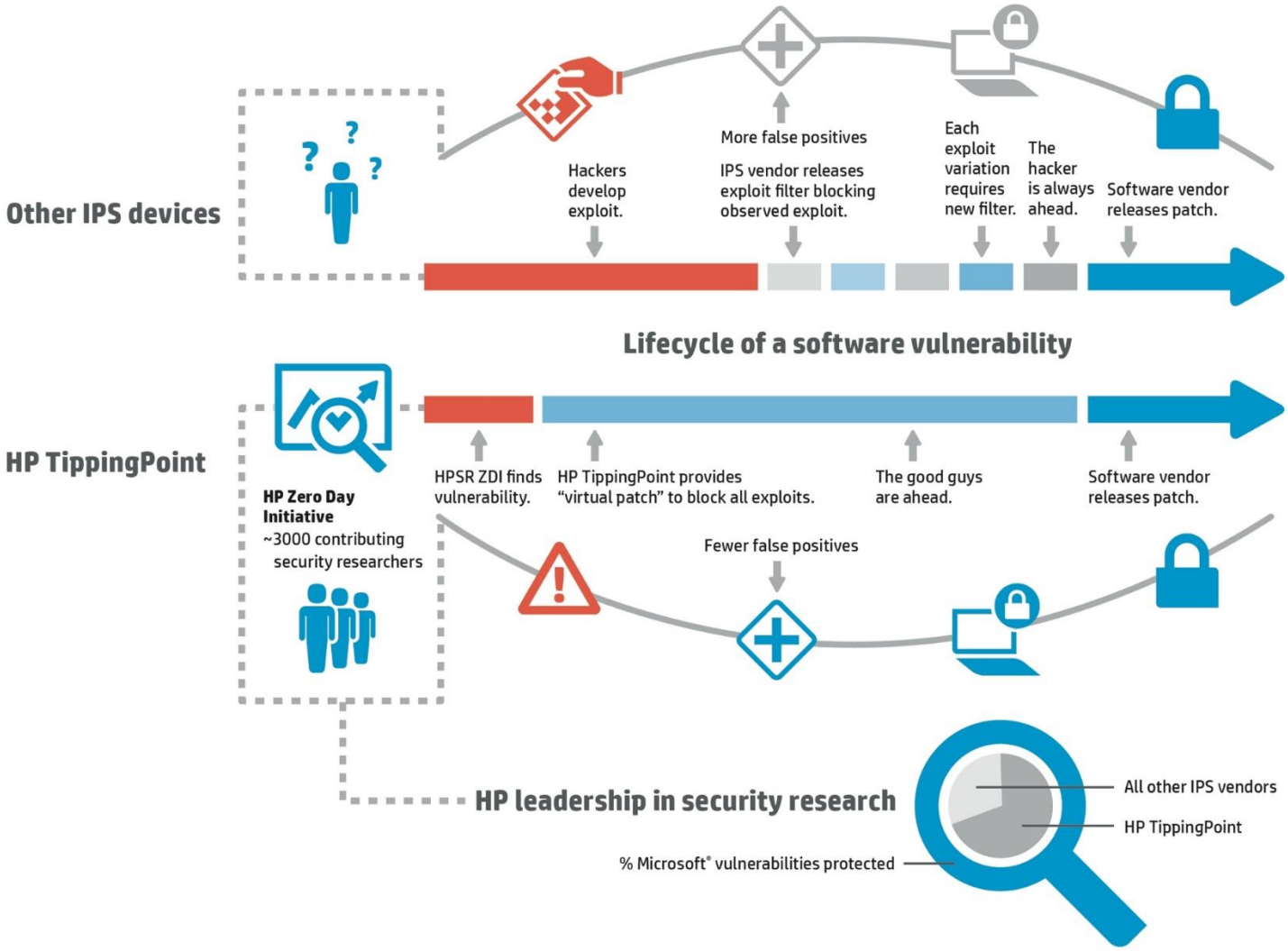
Кто такие DVLabs?



TIPPINGPOINT DIGITAL VACCINE LABS

- Разработка фильтров (DV)
- Обеспечение регулярного обновления всех типов сигнатур
- Взаимодействие с исследователями и производителями

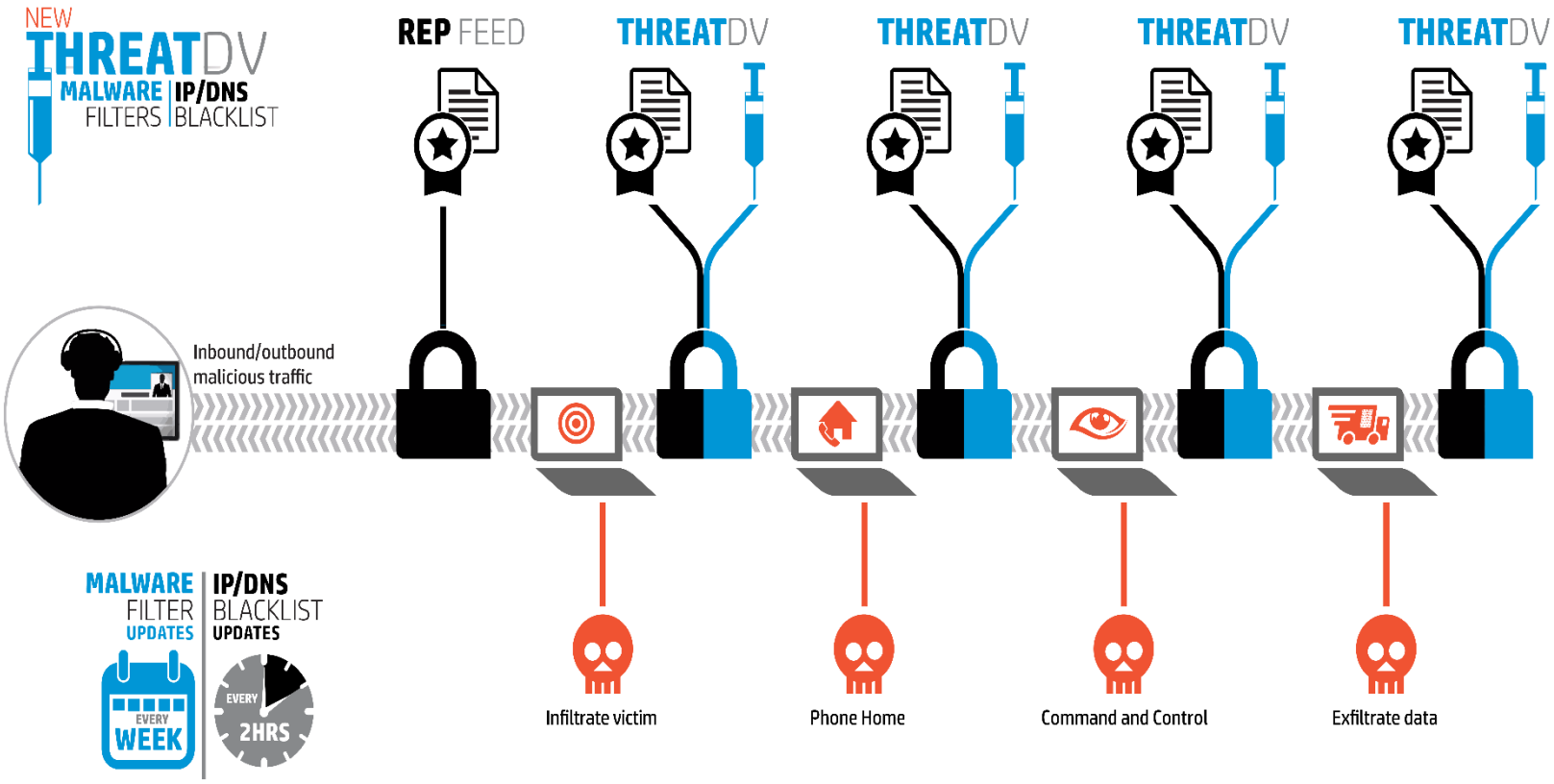
ZDI Инициатива «нулевого дня»



Что мы имеем на выходе?

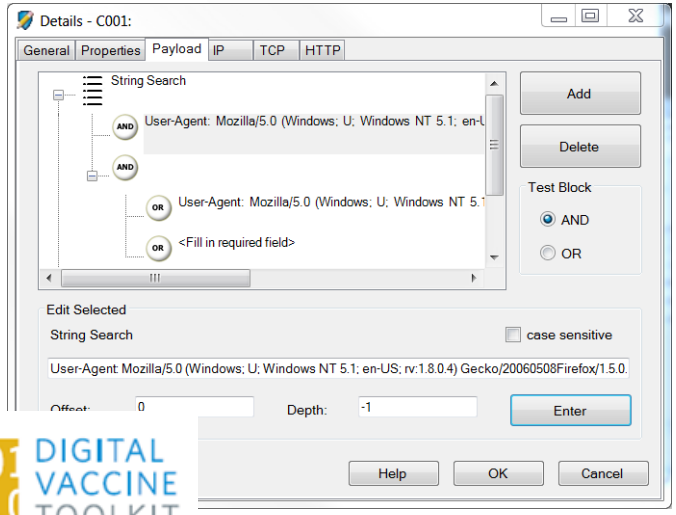
- Сигнатуры уязвимостей (Digital Vaccine)
- Сигнатуры ВПО (Malware Vaccine)
- Репутационные базы (RepDV Digital Vaccine)
- Анти-DoS/DDoS фильтры и профили
- Сигнатуры приложений (Application Visibility)

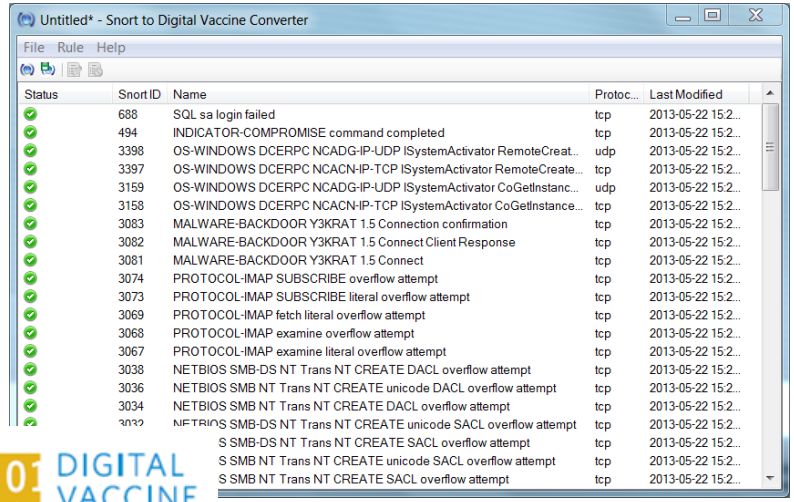
ThreatDV


NEW
THREATDV
MALWARE FILTERS
IP/DNS BLACKLIST
REP FEED
THREATDV
THREATDV
THREATDV
THREATDV
Inbound/outbound malicious traffic
MALWARE FILTER UPDATES
EVERY WEEK
IP/DNS BLACKLIST UPDATES
EVERY 2HRS
Infiltrate victim
Phone Home
Command and Control
Exfiltrate data

«Свои» сигнатуры

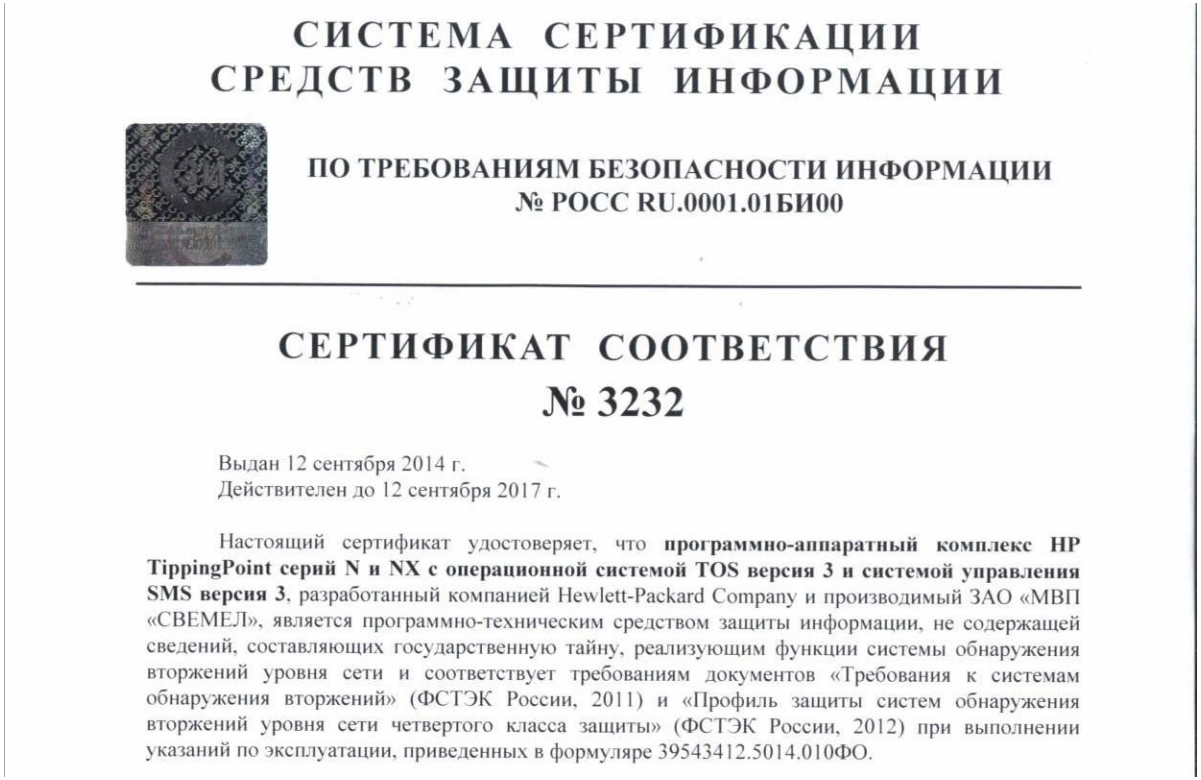
- Создание фильтров самостоятельно на основе анализа трафика (DV Toolkit)
- Импорт правил в формате SNORT (DV Converter)





Сертификация ФСТЭК

- Сертификат №3232 от 12.09.14г (НДВ-4, СОВ-4, 1Г, ИСПДн-1)
- Требования к системам обнаружения вторжений» (ФСТЭК России 2011)
- Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты» (ФСТЭК России 2012)



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3232

Выдан 12 сентября 2014 г.
Действителен до 12 сентября 2017 г.

Настоящий сертификат удостоверяет, что **программно-аппаратный комплекс HP TippingPoint серий N и NX с операционной системой TOS версия 3 и системой управления SMS версия 3**, разработанный компанией Hewlett-Packard Company и производимый ЗАО «МВП «СВЕМЕЛ», является программно-техническим средством защиты информации, не содержащей сведений, составляющих государственную тайну, реализующим функции системы обнаружения вторжений уровня сети и соответствует требованиям документов «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011) и «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты» (ФСТЭК России, 2012) при выполнении указаний по эксплуатации, приведенных в формуляре 39543412.5014.010ФО.

Итоги

- Защищает не от вирусов, а именно от взломов
- Высокая скорость реакции на новые угрозы с выходом сигнатур
- Высокая точность – наименьшее количество ложных срабатываний
- Высокая доступность за счет архитектуры
- Гибкий инструмент для большого кол-ва разных вариантов даже в пределах одного устройства
- Простота установки и простота настройки. Обучение админа по данной технологии – максимум 3 дня.

Вопросы?

Наумов Илья

117105, г. Москва, ул. Нагатинская, д. 1

Телефон: +7 (495) 980-67-76
Факс: +7 (495) 980-67-75

http://www.DialogNauka.ru
e-mail: ilya.naumov@DialogNauka.ru