KASPERSKY lab

ПРОТИВОДЕЙСТВИЕ ЦЕЛЕНАПРАВЛЕННЫМ АТАКАМ В УСЛОВИЯХ КОНВЕРГЕНЦИИ ТЕХНОЛОГИЙ РЫНКА АНТИ-APT РЕШЕНИЙ

Олег Глебов
Руководитель направления развития решений по противодействию целевым атакам и передовым угрозам

InfoSecurity Russia, 21 сентября, 2016 года

КАКИХ РЕШЕНИЯ ВЫ УЖЕ ЗНАЕТЕ?

«Рынок» анти-APT решений

AhnLab Damballa Fortinet McAfee CheckPoint

Cyphort PaloAlto Cisco AMP Triumfant TrendMicro

FireEye Fidelis KasperskyLab Last line Symantec

Group-IB Forcepoint CarbonBlack Huawei Cybertinel

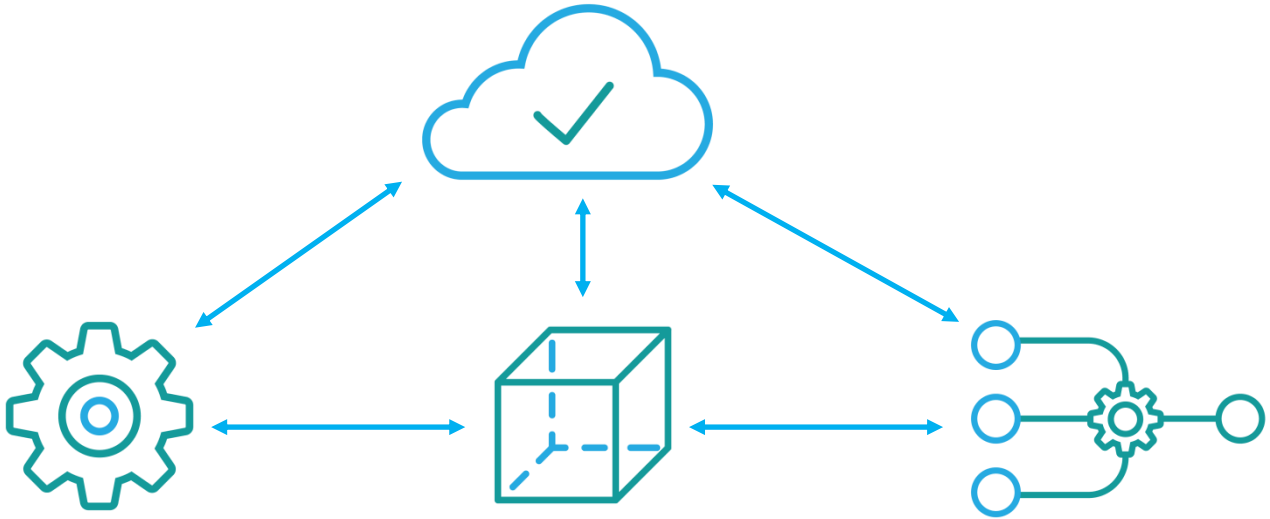
Attivo Networks StormShield Zscaler GuardiCore

Comodo LightCyber Guidance Software InfoWatch RSA

IDM/IGA PIM/PUM SIEM

ФУНКЦИОНАЛ ЗРЕЛОГО АНТИ-APT РЕШЕНИЯ

Глобальные репутационные сервисы и статистика угроз (Threat Intelligence)



Анализ аномалий сетевого трафика

HTTP/HTTPS/Mail/FTP/DNS sensors, endpoint agents

«Песочница»

Анализ объектов

Payload analysis

Анализ поведения рабочих станций

Process/configuration monitoring

РЕШЕНИЯ СЕТЕВОГО УРОВНЯ

	Предотвращение	Обнаружение	Реагирование
Сетевой уровень	Cisco	FireEye	BlueCoat
	Fortinet	Group-IB	
	CheckPoint	LastLine	RSA
	PaloAlto	Kaspersky Lab	

РЕШЕНИЯ УРОВНЯ РАБОЧИХ МЕСТ

	Предотвращение	Обнаружение	Реагирование
Сетевой уровень	Cisco	FireEye	BlueCoat
	Fortinet	Group-IB	
	CheckPoint	LastLine	RSA
	PaloAlto	Kaspersky Lab	
Уровень рабочих мест	McAfee		
	Symantec	Tanium	
	Kaspersky	CarbonBlack	
	TrendMicro	Mandiant	

КОНВЕРГЕНЦИЯ РЫНКА РЕШЕНИЙ АНТИ-APT

<table>
<tr><th></th><th>Предотвращение</th><th>Обнаружение</th><th>Реагирование</th></tr>
<tr><td rowspan="4">Сетевой уровень</td><td>Cisco</td><td>FireEye</td><td rowspan="2">Symantec (BlueCoat)</td></tr>
<tr><td>Fortinet</td><td>Group-IB</td></tr>
<tr><td>CheckPoint</td><td>LastLine</td><td rowspan="2">RSA</td></tr>
<tr><td>PaloAlto</td><td>Kaspersky Lab</td></tr>
<tr><td rowspan="4">Уровень рабочих мест</td><td>McAfee</td><td>CheckPoint; PaloAlto</td><td></td></tr>
<tr><td>Symantec</td><td colspan="2" rowspan="2">EDR market:
McAfee, Symantec, Kaspersky (2017), Tanium, CarbonBlack, Bromium…</td></tr>
<tr><td>Kaspersky</td></tr>
<tr><td>TrendMicro</td><td colspan="2">FIreEye (Mandiant)</td></tr>
</table>

KASPERSKY lab

ENDPOINT DETECT AND RESPOND (EDR)

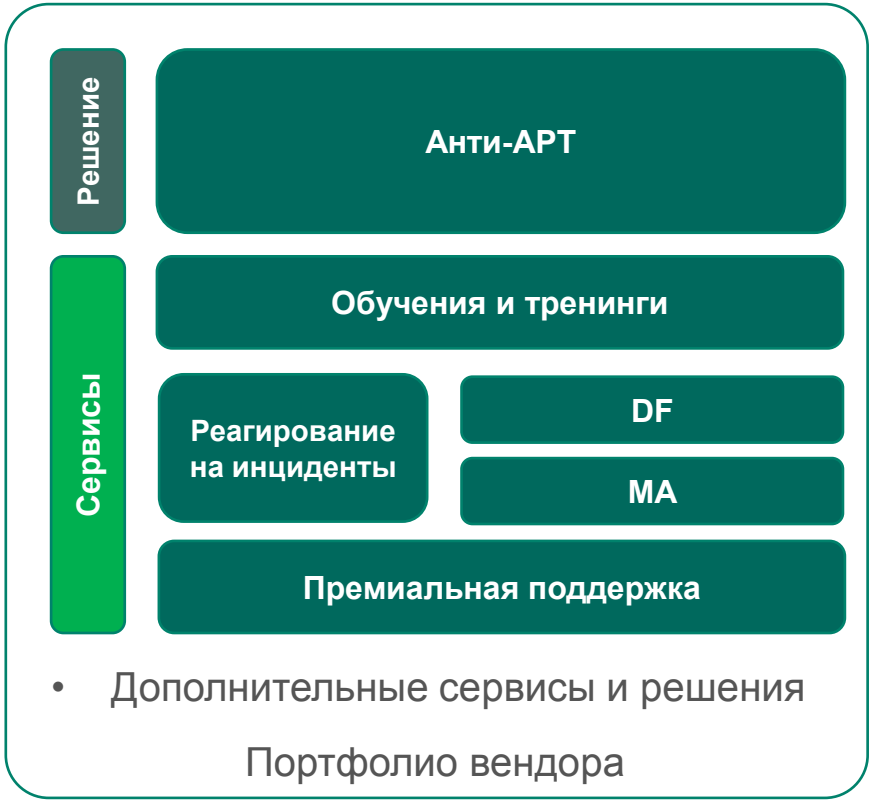
- **выявление инцидентов ИБ в момент их возникновения на рабочем месте**
  - нарушение политик ИБ
  - подозрительная/вредоносная активность
  - threat intelligence – выявление известных угроз
  - несанкционированное внесение изменение
  - ретроспективный анализ накопленной информации
  - динамический анализ потенциально опасных объектов с рабочих мест в выделенной «песочнице»
- **локализация инцидента в пределах масштаба на момент обнаружения**
  - предотвращение распространения угрозы средствами сторонних решений ИБ (например, антивирус/HIPS/DLP/HostFW)
  - карантинизация рабочего места
  - карантинизация объектов
  - отключение прав и привилегий скомпрометированных аккаунтов
- **поддержка проведения централизованных расследований инцидентов**
  - централизованный сбор необходимой информации с рабочих мест (дамп памяти, объектов,
  - централизованный «опрос» рабочих мест на предмет IOC или статическим скриптом («где ещё на рабочих местах есть _____?»)
  - хранение необходимой информации для ретроспективного анализа
- **предоставление механизмов реагирования на уровне рабочих мест подверженных атаке**
  - откат до прежнего состояния (roll back)
  - восстановление (repair)
  - удаление объектов, записей в реестре и тд.
  - Блокирование процессов и несанкционированных активностей

ВЫБОР РЕШЕНИЯ ДЛЯ ПРОТИВОДЕЙСТВИЯ ЦЕЛЕНАПРАВЛЕННЫМ АТАКАМ

- Общая оценка рынка (Gartner, Forrester, Radicati)
- Технологические тесты на эффективность детектирования у «песочниц» (NSS BDS, Miercom, ICSA Labs…)
- «независимые», «заказные» сравнения
- Battlecards
- Техническое задание

ОЖИДАНИЯ КОРПОРАТИВНЫХ ЗАКАЗЧИКОВ

ОЖИДАНИЯ VAD/ИНТЕГРАТОРОВ



- Дополнительные сервисы и решения

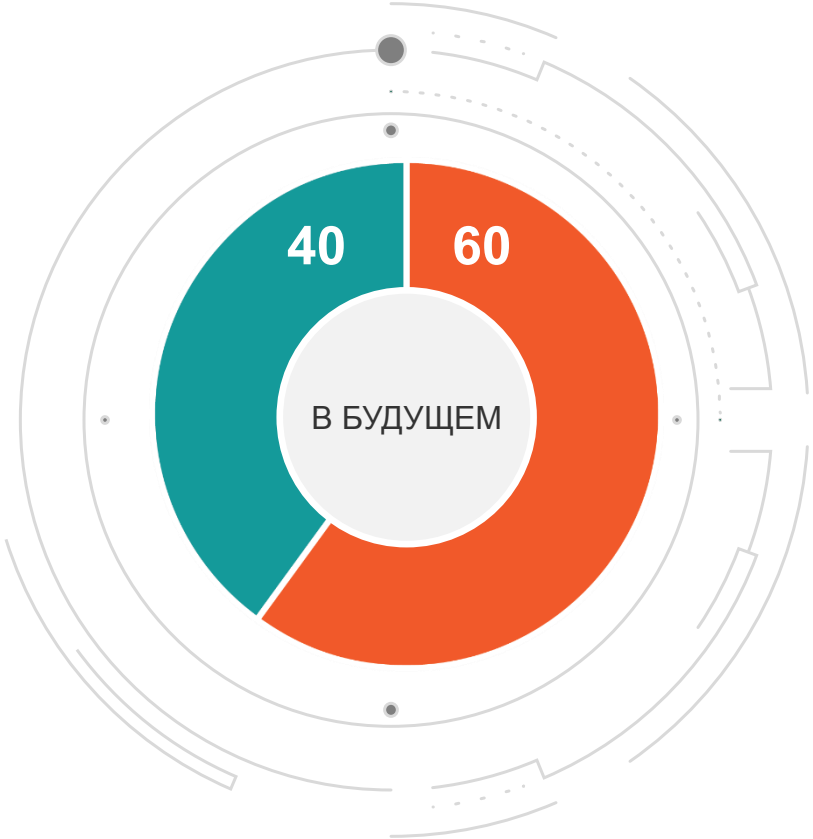
Портфолио вендора

Value Added Reseller

KASPERSKY lab

ЭВОЛЮЦИЯ ОЖИДАНИЙ БИЗНЕСА

- Текущий размер инвестиций: 80% на превентивные технологии / 20% на обнаружение, реагирование и прогнозирование (Крупные компании: 90%/10%)
- Планы опрошенных заказчиков на ближайшие 3 года: 40% / 60%
- Основано на опросе, проведенном «Лабораторией Касперского» в ноябре 2015 года среди свыше 6700 компаний по всему миру



KASPERSKY lab

РАЗВИТИЕ СТРАТЕГИИ ОБЕСПЕЧЕНИЯ ИБ

- Сигнатуры
- Точечные решения
- Статичный периметр контроля
- Владение = доверие
- Коробочные решения
- Ручная конфигурация политик
- Управление инцидентами
- Защита устройств
- **Блокирование и противодействие**

+

- Алгоритмы
- Решения корреляции и расшаривания данных
- Адаптивные периметры контроля
- Репутационные сервисы
- Автоматизация безопасности
- Постоянное реагирование
- Защита информации
- **Обнаружение и реагирование/расследование**

АДАПТИВНАЯ СТРАТЕГИЯ ПРОТИВОДЕЙСТВИЯ ПЕРЕДОВЫМ УГРОЗАМ ИБ

ПРОГНОЗИРОВАНИЕ

- Анализ потенциальных целей злоумышленников
- Управление уязвимостями
- Планирование развития стратегии защиты
- Создание адаптивного SOC

ПРЕДОТВРАЩЕНИЕ

- Снижение рисков проникновения
- Повышение эффективности решений и процессов ИБ
- Повышение осведомленности сотрудников

РЕАГИРОВАНИЕ

- Оперативное реагирование на инциденты ИБ
- Расследование природы атаки:
  - реконструкция
  - сбор доказательств
  - поиск скомпрометированных активов

ОБНАРУЖЕНИЕ

- Выявление попыток и фактов существующего проникновения
- Подтверждение и приоритезация событий ИБ

KASPERSKY lab

СПАСИБО!

Kaspersky Lab

www.kaspersky.com

Олег Глебов
Руководитель направления развития
решений по противодействию
целевым атакам и передовым угрозам

Oleg.Glebov@Kaspersky.com
D: +7 495 797 87 00 x5609
M: +7 910 476 94 10

https://ru.linkedin.com/in/glebovoleg

KASPERSKY lab