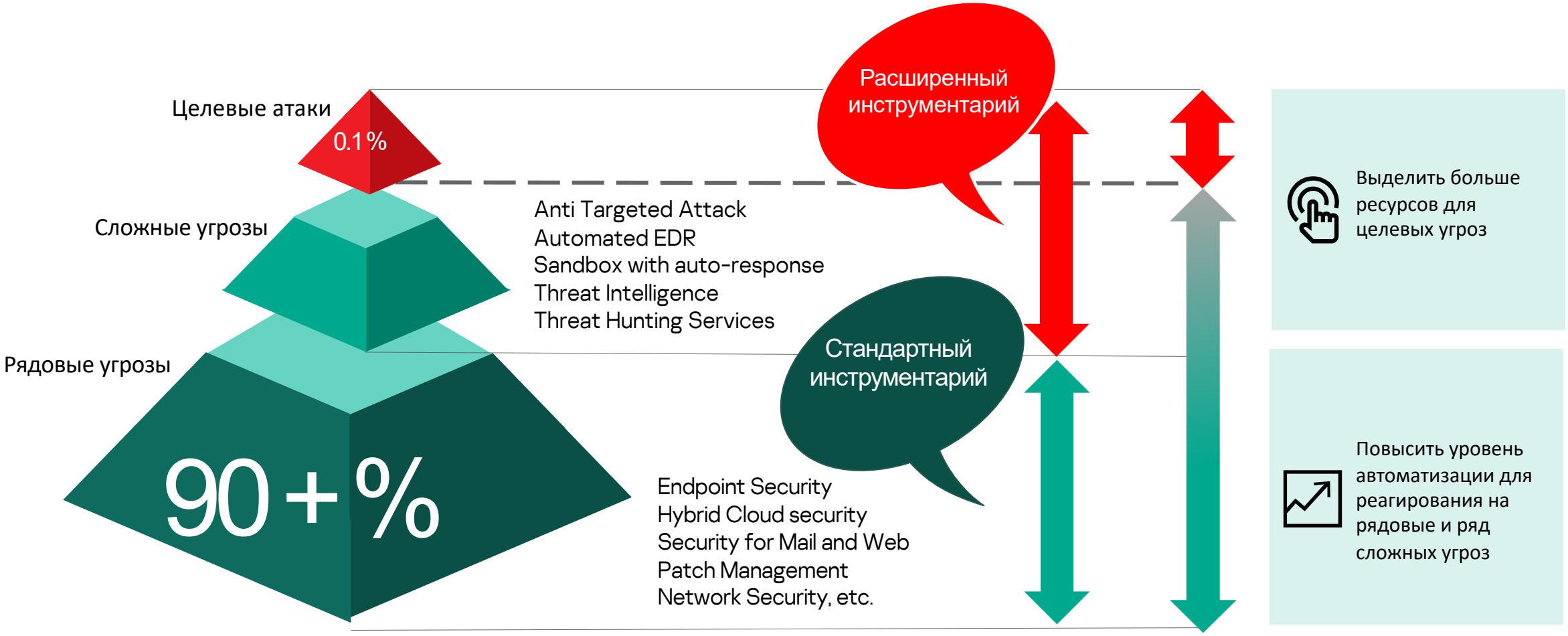
kaspersky

Технологические подходы к автоматизации реагирования на инциденты ИБ

Вениамин Левцов

Директор департамента корпоративного бизнеса
Лаборатория Касперского

Автоматизация реагирования на сложные угрозы, или Advanced Threats Protection (ATP) Automation



Важные вызовы информационной безопасности

- Prevent -> Detect: исследование подозрительных активностей
- Доступность продвинутых технологий для подготовки атак
- Недостаточность функции пост-мониторинга событий в SOC
- Ограниченность ресурсов ИБ и потребность в узких специалистах

kaspersky

Подходы к обеспечению большей автоматизации реагирования на сложные угрозы

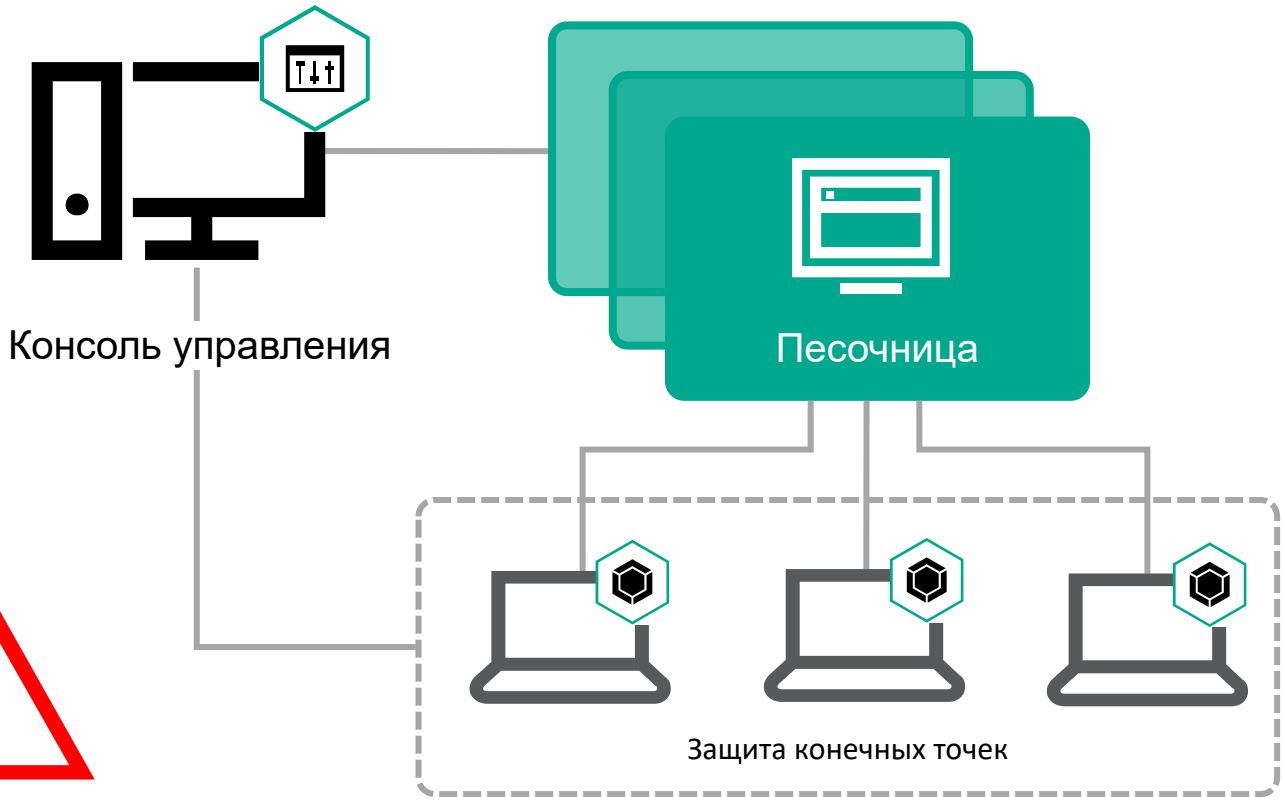
Поведенческий анализ сложных и новых угроз

Классы угроз

- Шифровальщики
- Ранее неизвестное ВПО
- ПО, использующее уязвимости нулевого дня
- Легитимное ПО
- Fileless malware
- Элементы APT

Важные особенности

- Отдельный сервер «песочницы»
- Связь с превентивным средством
  - Защита конечной точки
  - Почтовый или web шлюз
- Политики автоматического реагирования
- Собственная разработка производителя



EDR (Detection and Response): автоматизированное сканирование хостов

Автоматизированный поиск совпадений по индикаторам:
регулярные проверки, условные по событию или по расписанию

IoC

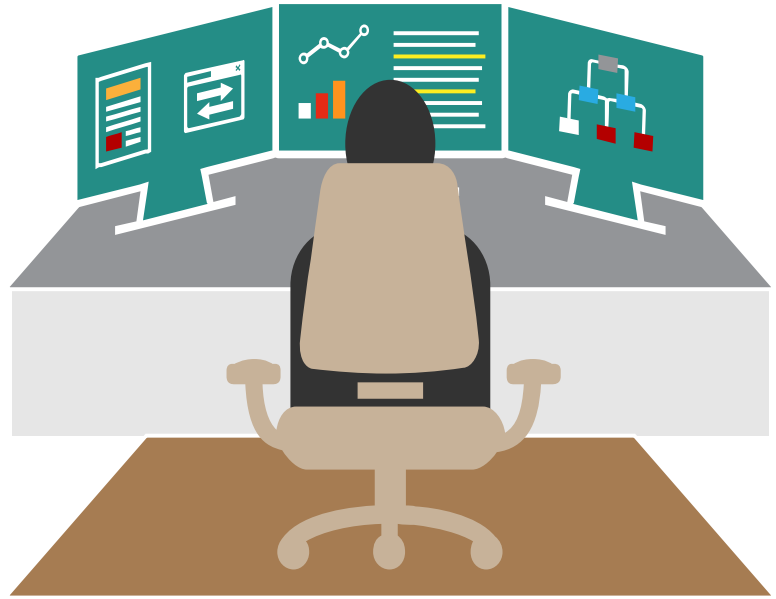
- Получение индикаторов из различных источников Threat Intelligence
- Обнаружение отдельных признаков инцидента
- Ретроспективный поиск по хранилищам

IoA

- Получение индикаторов из надежной базы производителя
- Обнаружение набора элементов и автоматическое подтверждение факта инцидента
- Возможность использовать список рекомендаций для реакции на инцидент
- Соответствие классификации MITRE ATT&CK
- Создание собственных индикаторов IoA

Использование потоков данных об угрозах, или Threat Data Feeds

- Malicious and Phishing URL feeds
- Malicious URL Exact Data Feed
- Phishing URL Exact Data Feed
- Ransomware URL Feed links and websites that host ransomware
- Botnet C&C URL Feed
- Botnet C&C URL Exact Data Feed
- Mobile Botnet C&C URL Data Feed
- Malicious Hash Feed
- ICS Hash Feed –specific for Industrial Control Systems (ICS)
- P-SMS Trojan Feed
- IP Reputation Data Feed
- IoT URL Data Feed
- APT Hash Data Feed
- APT IP Data Feed
- APT URL Data Feed
- Vulnerability Data Feed



Actionable Threat Intelligence Ingesting:

- SIEM
- EDR
- Web/Mail Шлюз
- Threat Intelligence Platform

Новые технологии:
Обнаружении элементов атаки по схожести кода приложений

Пример кооперации различных систем обнаружения и реагирования

Технический состав атаки:

- Средствами корпоративной или web- почты доставляется файл Microsoft Office, содержащий макрос
- Макрос запускает PowerShell команду для установления связи с C&C сервером
- И загружает файлы на доступный в скомпрометированной сети Samba сервер
- Запускается скрипт сетевой разведки и поиска уязвимых для удаленного запуска приложений узлов сети
- На обнаруженных узлах при помощи PsExec запускает команды загрузки и запуска ВПО с Samba сервера

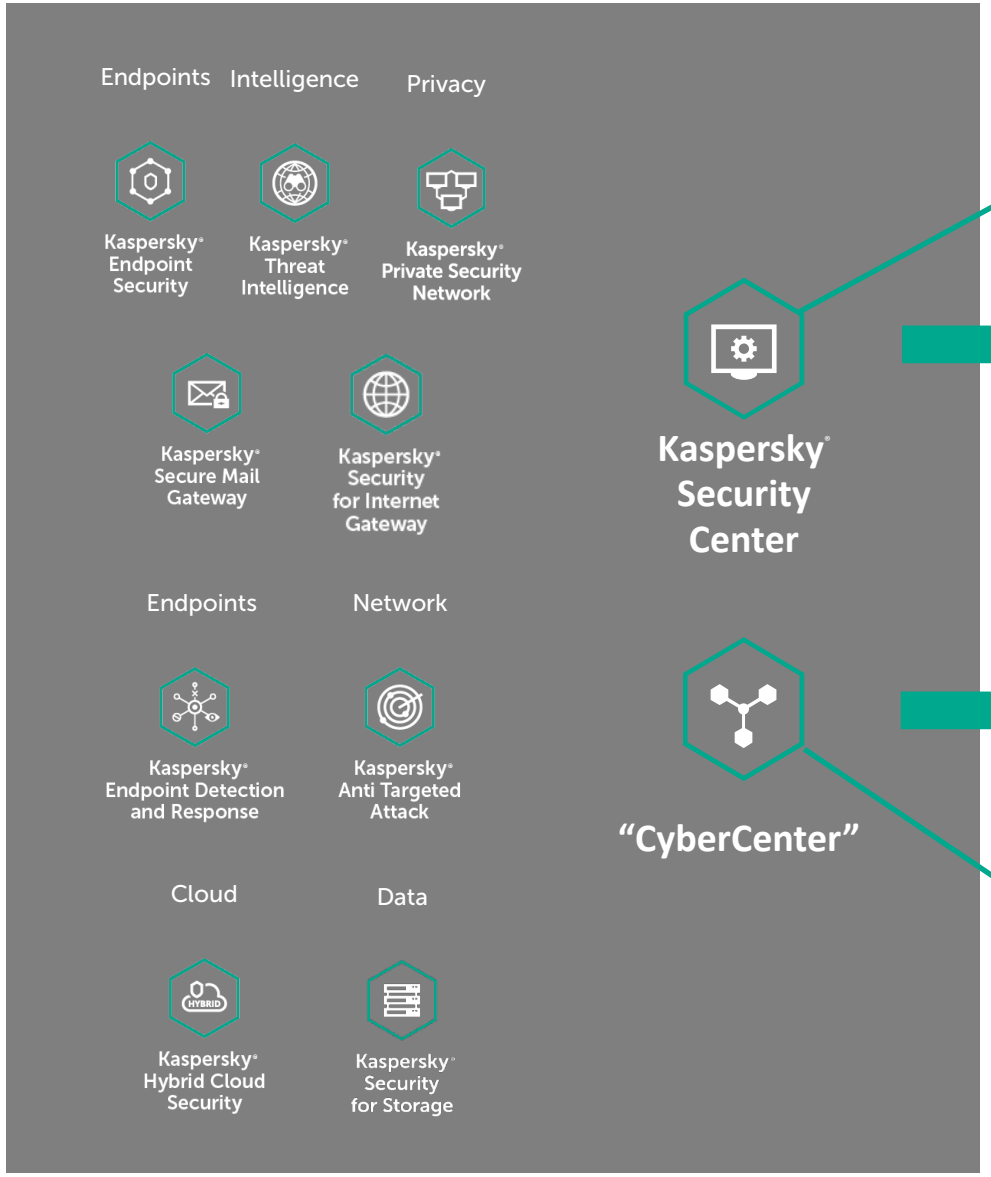
Средства обнаружения элементов атаки и обнаруженные вредоносные активности:

- Threat Feed (C&Cs) интегрированный с SIEM/Gateway – соединение с известным C&C сервером;
- EDR – обнаружение вызова PowerShell программой из пакета Microsoft Office;
- EDR - срабатывает IoA на запуск соединений на порты, используемые при экплуатации уязвимостей и удаленном запуске приложений;
- EDR – срабатывает IoA на средства сетевой разведки (команды ping, arp, telnet);
- Sandbox – анализирует поведение приложения, загруженного с C&C сервера

Комплекс мер по автоматической реакции:

- Правило в SIEM – формируется IoC на параметры хоста C&C и запускает поиск по журналам событий;
- EDR – проводит сканирование узлов сети по индикаторам C&C и hash файла, скачанного с C&C сервера;
- EDR – создается автоматическое правило блокировки запуска файлов, относящихся к данной атаке;
- EDR – (дополнительно) производится блокировка сетевых соединений на зараженных узлах сети;
- Mail gateway + Sandbox + SIEM – формируется автоматическое правило реакции на письма с e-mail.

На пути к SOAR - Security Orchestration, Automation and Response платформе

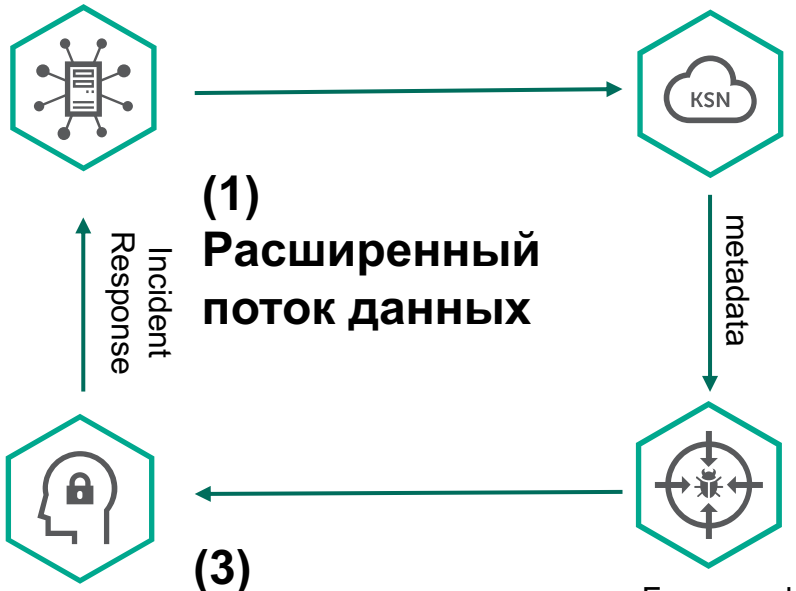


Администрирование продуктов

- Обнаружение угроз на основе событий различных решений (cross-products)
- Расширенная телеметрия от продуктов
- Единая картина обнаружений от различных источников (PCs, Mobiles, Cloud, Web, etc)
- Расширенные механизмы обнаружения
- Trigger -> Validation -> Auto-Response
- Политики автоматического реагирования (pre-defined playbooks)
- Enforcement tools (EDR, gateway)
- Машинное обучение для категоризации и определения критичности инцидентов
- Установка в сети заказчика

Сервисы управления информационной безопасностью: детектирование сложных угроз

Рабочее место с продуктом ИБ



Глобальная сеть производителя решения

(1)
Расширенный поток данных

Команда ИБ заказчика

Центр Threat Hunting, инфраструктура и команды аналитиков

Framework
- 24x7
- 5x8

(2)
Анализ данных:
- **На основе Threat Intelligence**
- **Машинное обучение**
- **Сценарии MITRE**
- **Собственные IoA**
- **Экспертный анализ**

(3)
Отчеты
- **регулярные**
- **срочные**

Сервисы управления информационной безопасностью: автоматизированное реагирование на инциденты (MDR)

Набор решений и EDR

Механизмы обнаружения сложных угроз

Статус инцидента (портал) и коммуникации с экспертами SOC

Guided Automated Response Playbooks

SLA

Экспертные расследование для сложных инцидентов

Передаваемая технология MDR для

- MSSP,
- служб ИБ крупных организаций
- Национальных проектов

Подходы к автоматизации поиска и реагирования на сложные угрозы

kaspersky

Вопросы

Вениамин Левцов
Veniamin.Levtsov@Kaspersky.com

kaspersky.com