Kaspersky
Security Day
2021

Kaspersky Expert Security:

от отдельных решений – к комплексной системе защиты от киберугроз

Вениамин Левцов,
директор департамента
корпоративного бизнеса

kaspersky

От защиты конечных точек — к информационной безопасности компании

Инфраструктура

Сложные угрозы

Экспертные сервисы

SOC

Концепция Security Frameworks

Сложность угроз	Размер организации. Зрелость команды ИБ	Пакеты решений	Основные продукты «Лаборатории Касперского»
Угрозы национального уровня	CERT — Экспертная команда	National Cybersecurity	• Содействие национальным органам • Построение национального SOC
Целевые атаки и взломы	2500+ — Служба ИБ	Kaspersky Expert Security	Kaspersky Anti Targeted Attack Platform; Kaspersky Endpoint Detection and Response; Kaspersky Threat Intelligence; Kaspersky Unified Monitoring and Analysis Platform
Сложные угрозы	500-2500 — Выделенные сотрудники ИБ	Kaspersky Optimum Security	Kaspersky Sandbox; Kaspersky Endpoint Detection and Response Optimum; Kaspersky Security Awareness; Kaspersky Managed Detection and Response
Базовые угрозы	<500 — ИТ	Kaspersky Security Foundations	Kaspersky Endpoint Security for Business; Kaspersky Hybrid Cloud Security; Kaspersky Security for Mail Server; Kaspersky Security for Internet Gateway

Профиль заказчика

- Более 1000 рабочих мест в сети
- Сформирован Департамент ИБ
- Налажены процессы реагирования на инциденты ИБ
- SIEM используется или планируется к внедрению
- Регулярно проводятся внешние тесты защищенности
- Часто: имеется индустриальная сеть

Современные реалии рынка ИБ

- Соответствие регуляторным требованиям
- Растущая сложность и интенсивность угроз
- Разнородность систем ИБ
- Нехватка сотрудников

Наш ответ на вызовы для ИБ (1): технологии распознавания угроз

Дополнительные технологии распознавания угроз

- Расширенный анализ поведения – песочницы
- Анализ происхождения исходного кода – сравнение с «генами» известных угроз
- Данные об угрозах – потоки, или фиды для автоматического применения (MRTI), отчеты, поисковые порталы
- Проверка на совпадение со структурированным списком известных техник, приемов и тактик атак – MITRE ATT&CK®

Подробнее

Command and Scripting Interpreter

Техника T1059

Описание	Использование легитимных интерпретаторов (PowerShell, Perl, Python) для выполнения вредоносной активности
Использование	Загрузка вредоносного скрипта легитимным приложением через встроенную функциональность (макрос)
Правило детекта	Обнаружение факта загрузки интерпретируемых (исполняемых) файлов офисными приложениями
Техника детекта	Мониторинг сетевых соединений в системе с привязкой к конкретным процессам, инициировавшим подключение
Логика работы	Правило отслеживает обращение процессов Microsoft Access / Excel / PowerPoint / Visio / Word к ссылкам, ведущим на исполняемые файлы (детект по расширению файла)

https://attack.mitre.org/techniques/T1059/

Create or Modify System Process

Техника T1543

Описание	Для обеспечения присутствия на атакуемой системе злоумышленники могут изменять поведение системных процессов/служб, чтобы обеспечить запуск вредоносных компонентов
Использование	Например, через правку системного реестра удается переопределить поведение системы и добиться запуска «полезной нагрузки» при падении той или иной службы ОС
Правило детекта	Мониторинг активности в системном реестре (создание/модификация/удаление ключей реестра)
Техника детекта	Отслеживание изменение значений ключа (параметра), который определяет поведение системы в случае падения конкретной службы

https://attack.mitre.org/techniques/T1543/

Экспертные сервисы кибербезопасности

Kaspersky Security Assessment

Поиск следов атак и вредоносных активностей в сети

Kaspersky Incident Response

Обнаружение и устранение последствий инцидентов кибербезопасности

Подписка

Kaspersky Managed Detection and Response

Мониторинг потока телеметрии от конечных точек

Kaspersky Endpoint Detection and Response

Поддержка поставщиков сервисов ИБ: KEDR как инструмент MSSP

Наш ответ на вызовы для ИБ (3): автоматизация с использованием SIEM платформы

Kaspersky Unified Monitoring and Analysis Platform

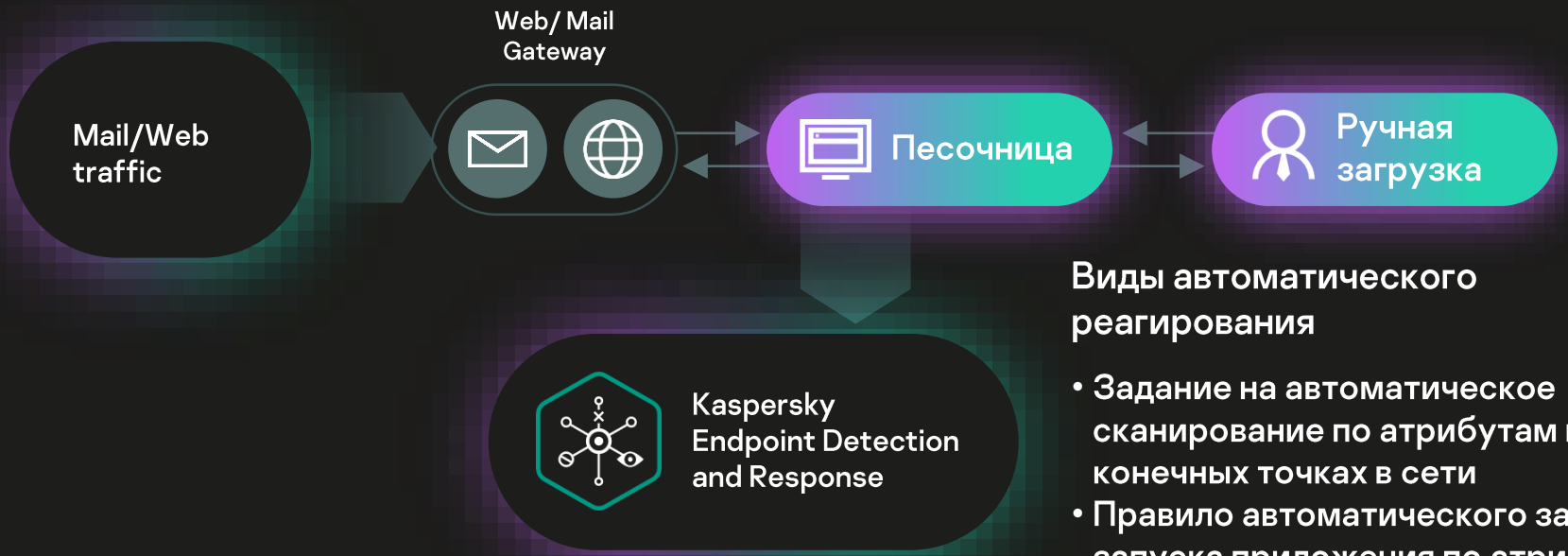
- Запросы собственной службы ИБ, приобретение команды разработки
- Высокая производительность
- Модульность, микросервисность – гибкость использования под разные задачи
- Интегральная связанность с другими продуктами ЛК
- Встроенный движок Threat Intelligence
- Возможность автоматических проверок по контролам и поддержка концепции XDR

Целевая архитектура SOC на базе решений Лаборатории Касперского

Наш ответ на вызовы для ИБ (4): интеграционное взаимодействие различных решений

- Классический антивирус был «черным ящиком» – полный цикл реагирования на угрозу
- Повышение сложности угроз, вовлечение профессионалов «на той стороне» – появление инструментария для расследования
- Рост сложности инфраструктуры – разнородность решений ИБ, их политик и данных
- В фокусе: повышение операционной эффективности и мотивации службы ИБ

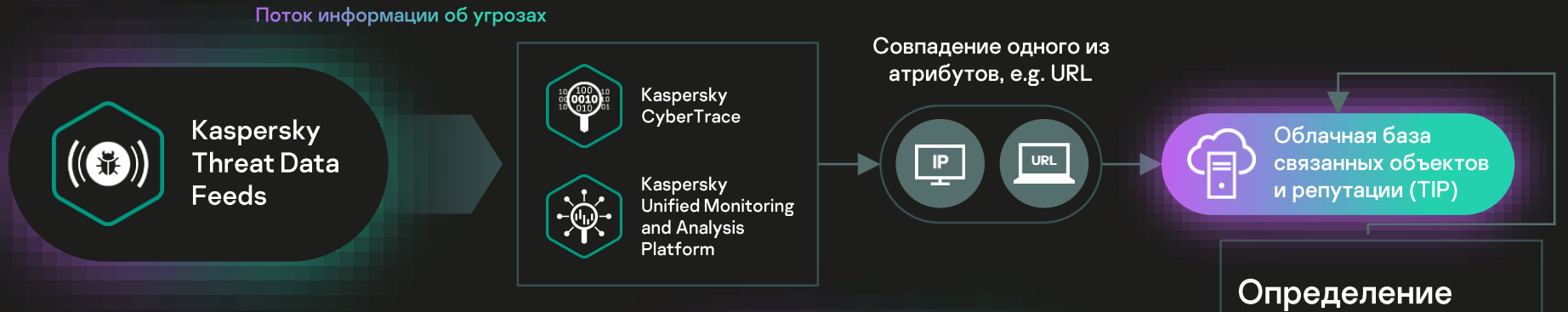
1 Запуск автоматических проверок



Виды автоматического реагирования

- Задание на автоматическое сканирование по атрибутам на конечных точках в сети
- Правило автоматического запрета запуска приложения по атрибутам

2 Обогащение связанными атрибутами



Виды автоматического реагирования

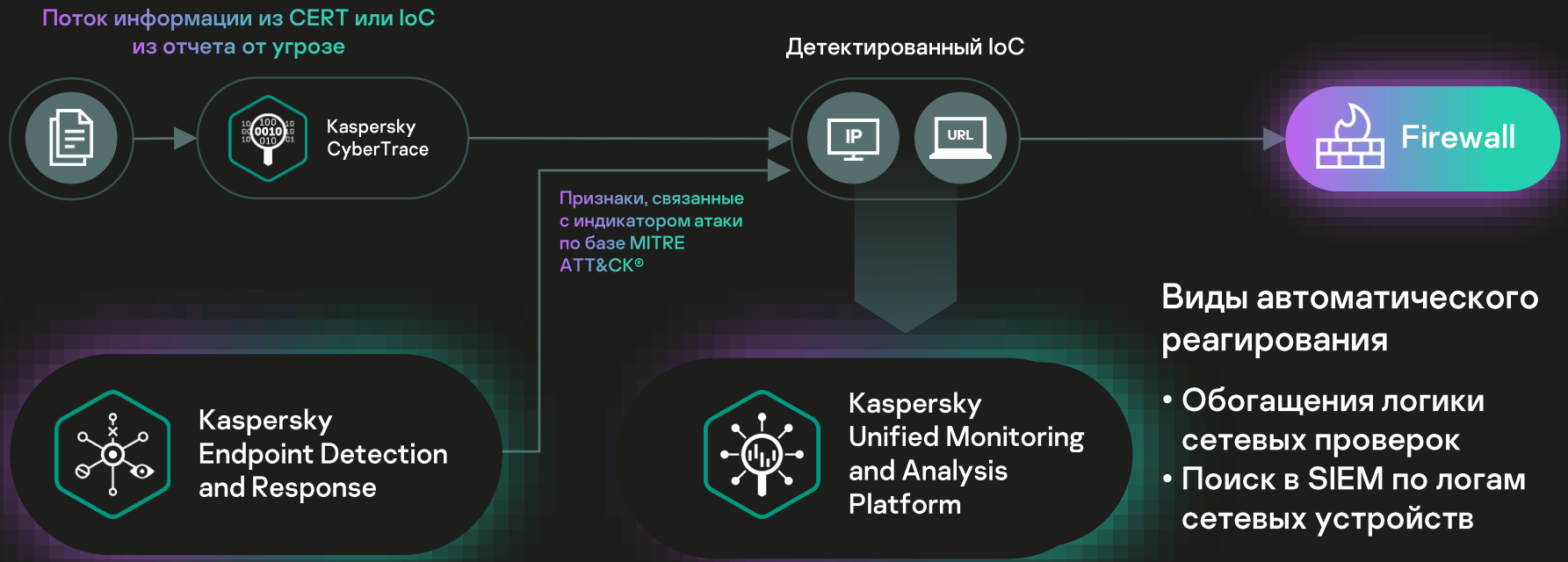
- Задание на автоматическое сканирование по атрибутам на конечных точках в сети
- Правило автоматического запрета запуска приложения по атрибутам
- Создание правила по поиску в логах на SIEM

Kaspersky Endpoint Detection and Response

Определение полного множества связанных атрибутов

URL, e-mails, домены того же хозяина, связанные hash / IoC, CVEs

3 Обращение к сетевым решениям

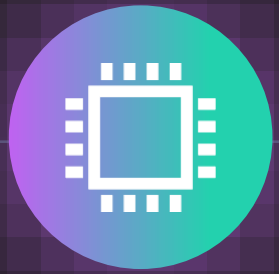


Виды автоматического реагирования

- Обогащения логики сетевых проверок
- Поиск в SIEM по логам сетевых устройств

Пути расширения возможностей реагирования на угрозы ИБ

Инвестиции в службу ИБ



Внешние сервисы ИБ (MSP / MSSP)

Концепция XDR

Внедрение инструментов и политик расширенного обнаружения угроз и автоматического или «ведомого» реагирования

> machines should work;
> people should think.

IBM Pollyanna Principle

Подробнее

Спасибо!

kaspersky