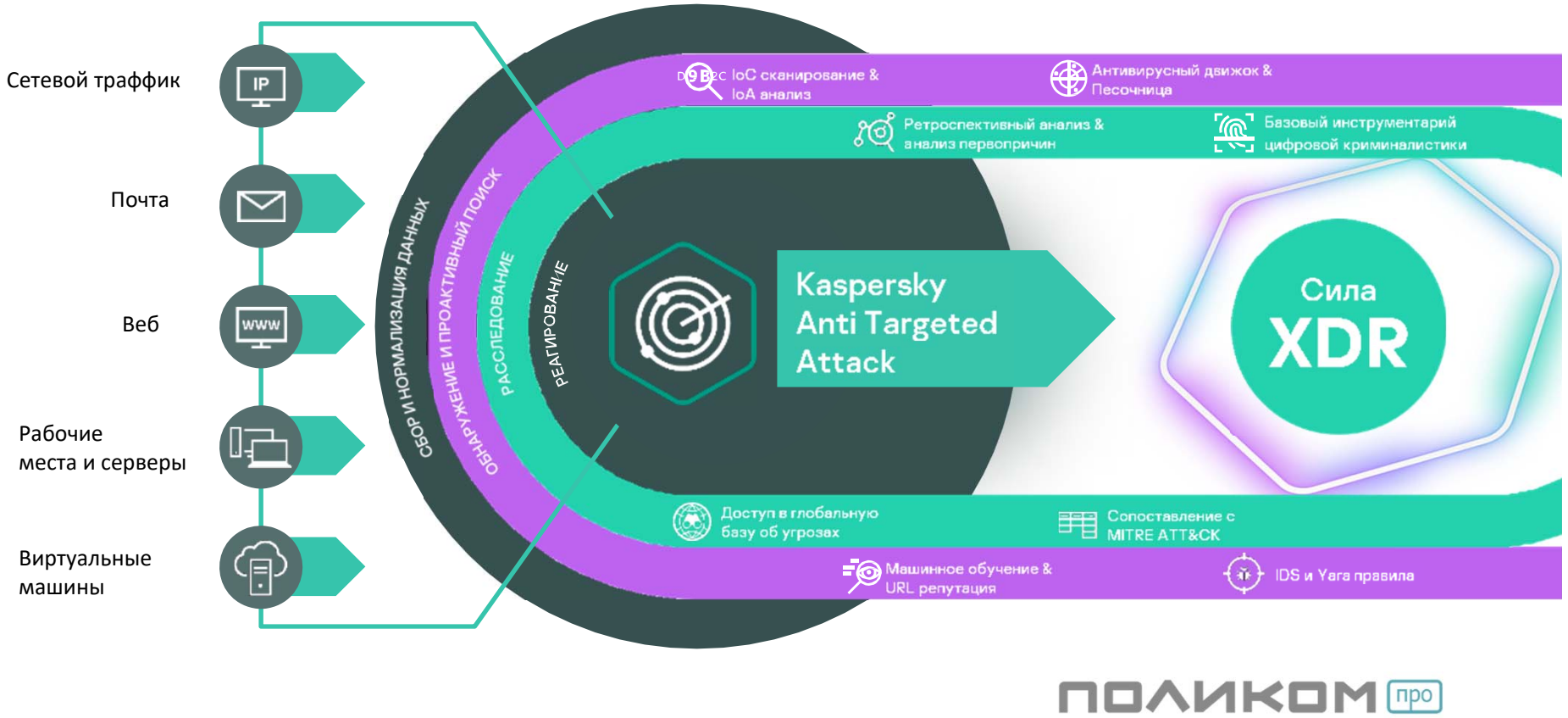
Kaspersky
Anti Targeted Attack

ПОЛИКОМ про

Платформа KATA с EDR: Расширенные возможности защиты XDR

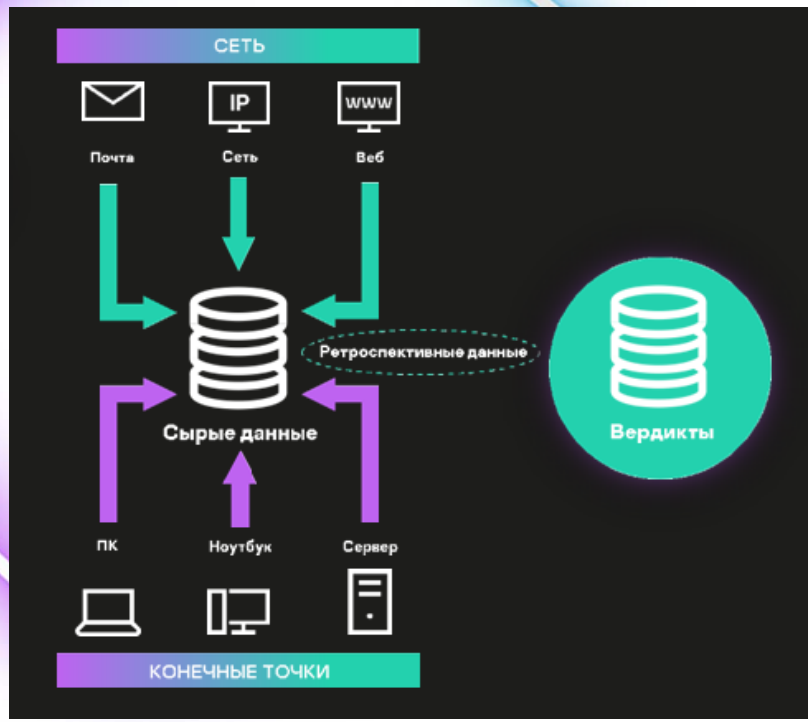


ПОЛИКОМ про

Автоматический сбор и централизованное хранение данных

Сбор и хранение

- Автоматический сбор, запись и хранение телеметрии/объектов/вердиктов
- Предоставляет необходимую информацию об Обнаруженных угрозах, облегчая работу ИБ-специалистов
- Предоставляет доступ к ретроспективным данным, Необходимым при проведения расследования при Недоступности или заражении рабочих станций или шифровании данных злоумышленниками
- Проактивный поиск угроз
- Позволяет расследовать продолжительные атаки и предоставляет группе реагирования и регулирующим органам своевременную информацию об обнаруженных инцидентах



ПОЛИКОМ про

Обнаружение угроз и информирование об угрозах

Обнаружение

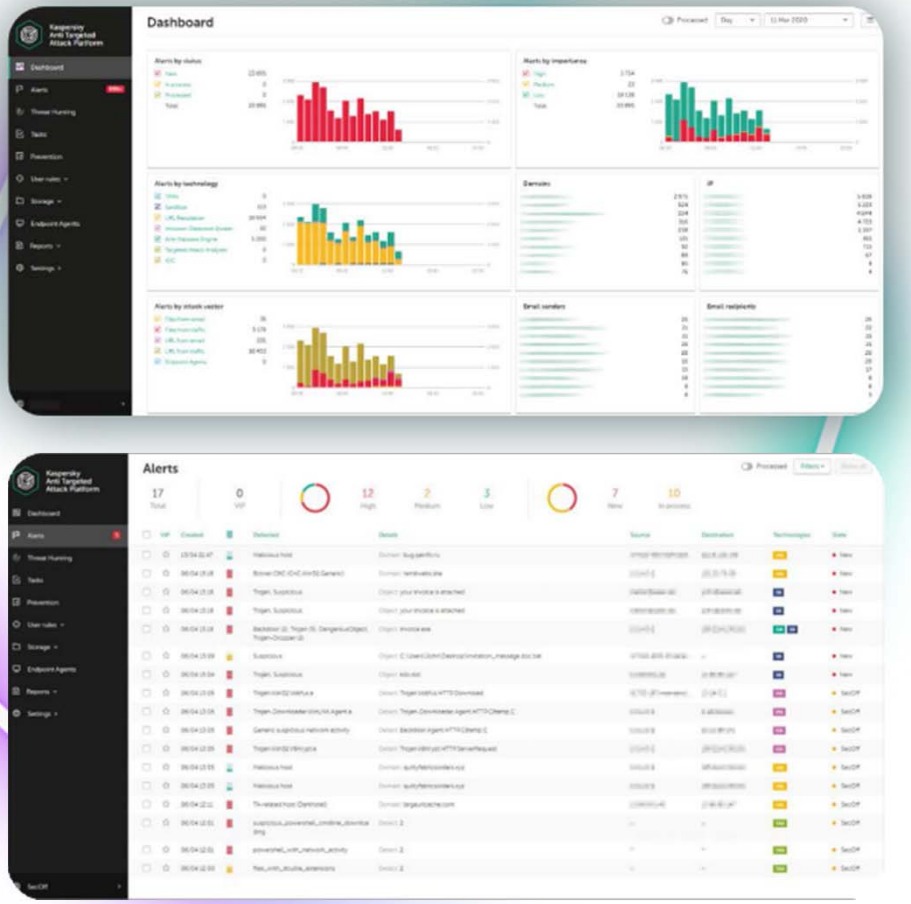
Большое количество детектирующих движков как для сети, так и для конечных точках

Сканирование инфраструктуры на наличие индикаторов компрометации

Работа над анализом индикаторов атак и сопоставление с MITRE ATT&CK

Передовая песочница

Рекомендации по расследованию и реагированию

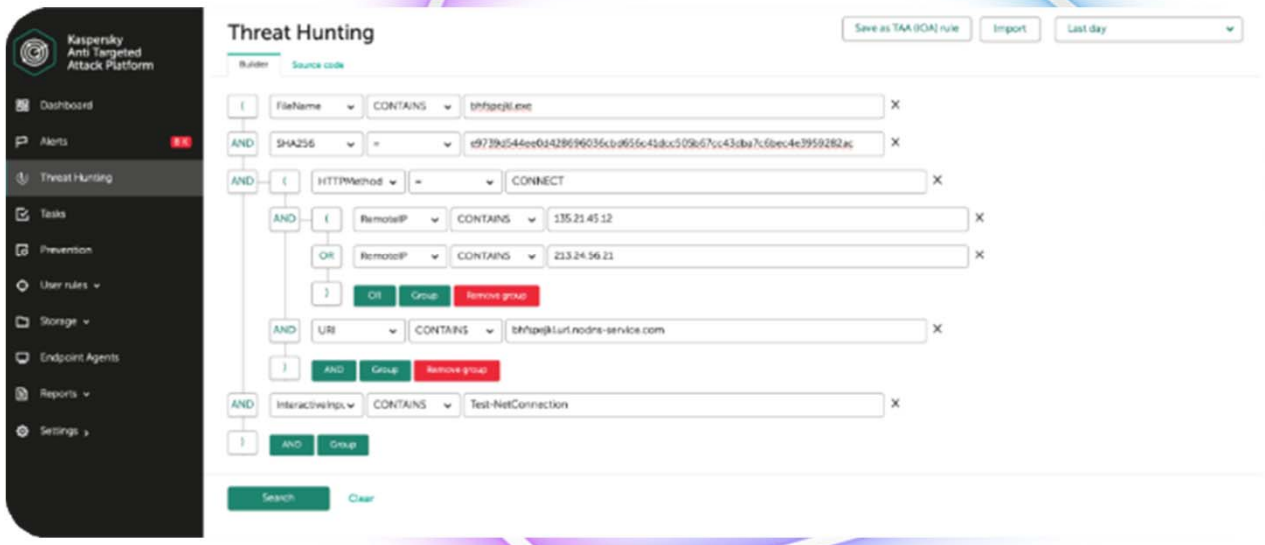


ПОЛИКОМ про

Проактивный поиск угроз (Threat Hunting)

Поиск угроз

- Удобный построитель запросов
- Ретроспективный поиск по телеметрии
- Предустановленные командлеты
- Логические операнды
- Автоматическая нормализация
- Визуализация цепочек событий



Повысить вероятности раннего обнаружения действий киберпреступников

Составлять сложные запросы на поиск нетипичного поведения, подозрительных активностей, или иных вредоносных действий

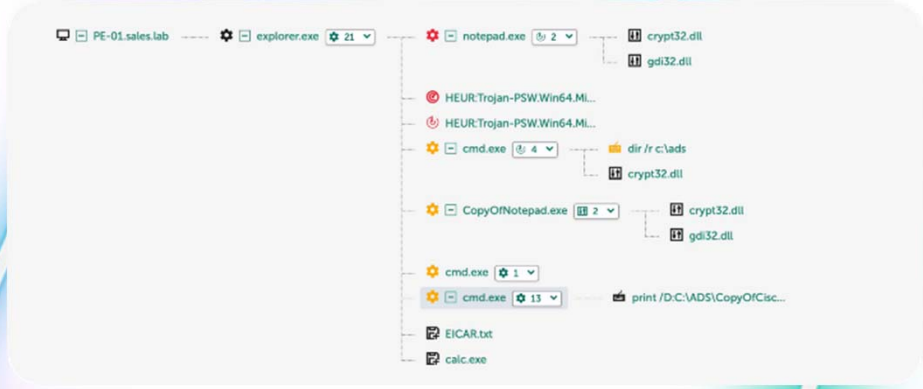
Поиск по техникам MITRE ATT&CK

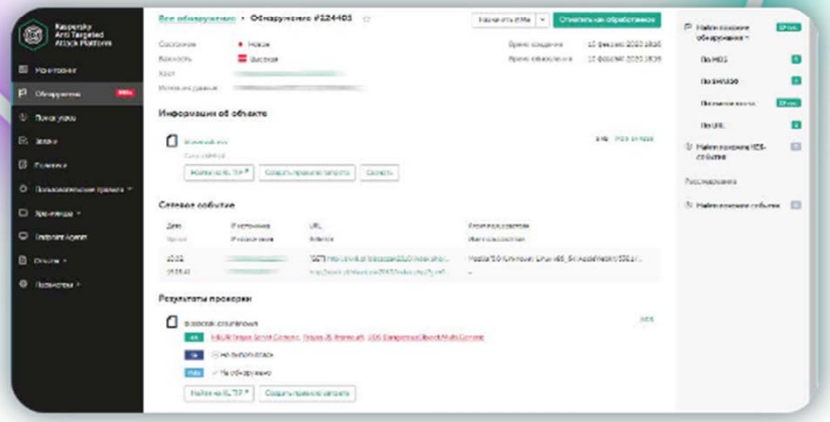
Учитывать в поиске особенностей и специфике защищаемой инфраструктуры

Детальное расследование инцидентов

Расследование

- Расширенные возможности анализа первопричин
- Рекомендации по расследованию
- Работа с порталом Kaspersky Threat Int elligence
- Сопоставление событий с глобальной базой знаний тактик и техник MITRE ATT&CK
- Обогащение подозрительных событий понятным описанием, трактовкой, примерами и рекомендациями по противодействию
- Ретроспективный анализ

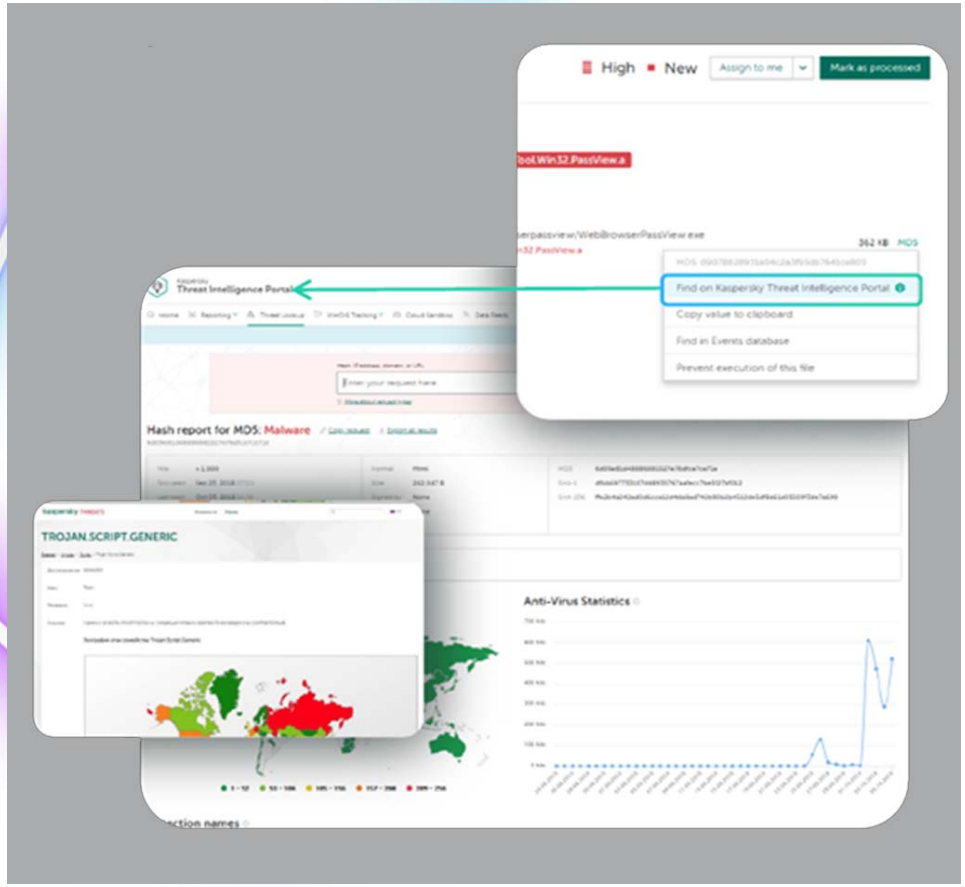




Взаимодействие с глобальной аналитикой киберугроз

Обогащение

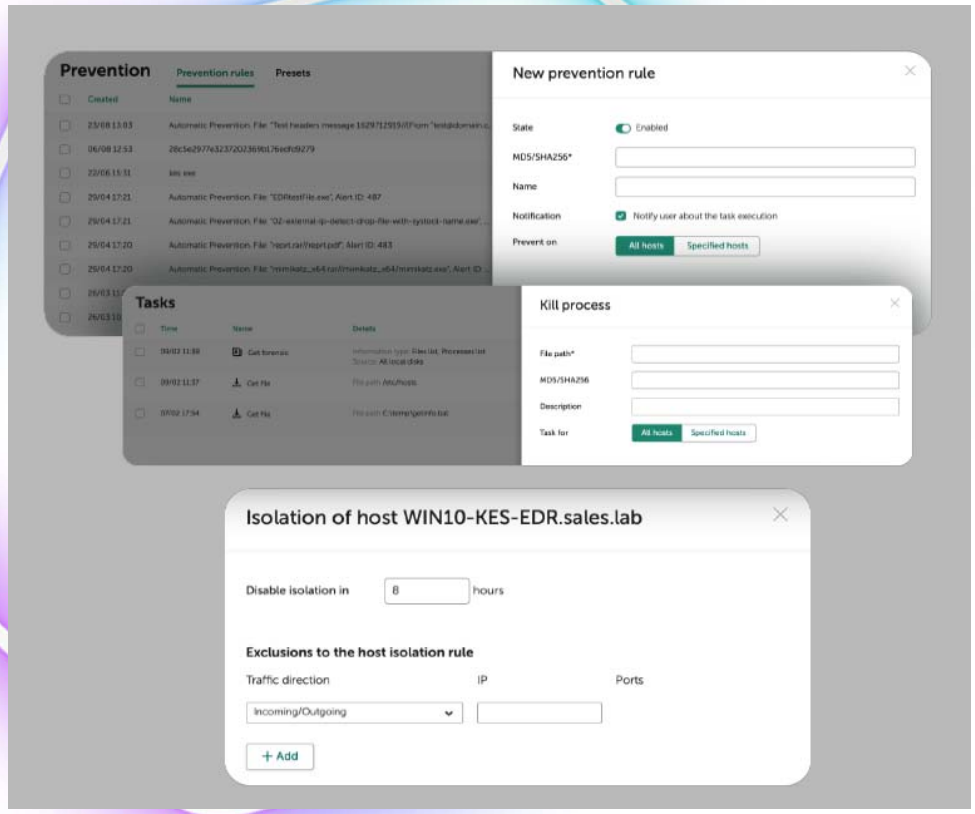
- Встроенный доступ к Kaspersky Threats
- Обогащение данными с матрицы MITRE ATT&CK
- Доступ на портал Kaspersky Threats Lookup
- Проведение запросов по угрозам вручную по базе данных
- Получение дополнительных данных для проактивного поиска угроз и проведения детального расследования инцидентов
- Непосредственный доступ к базе знаний через веб-интерфейс KATA/KEDR
- 1000 запросов в год включено в лицензию



Реагирование на инциденты

Реагирование

- Изолировать холст
- Остановить процесс
- Удалить файл
- Переместить файл в карантин
- Выполнить команду
- Создать превент правило
- Базовый инструментарий цифровой криминалистики
- Рекомендации по реагированию



ПОЛИКОМ про

Основные преимущества Платформы KATA с EDR

Один программный продукт с единой веб-консолью

Предоставляет комплексный единый инструментарий защиты

Защищает множество точек входа потенциальной атаки

Создает целостную картину происходящего

Автоматизирует рутинную ручную работу

Оптимизирует рабочую нагрузку экспертов

Уменьшает количество ложных срабатываний и время для анализа

Сокращает среднее время обнаружения на инциденты (MTTD/MTTR)

Повышает эффективность процесса реагирования на инциденты

ПОЛИКОМ про

kaspersky
Platinum Partner

Благодарю за внимание!

Руководитель направления решений
«Лаборатории Касперского»
Михаил Усачёв

тел: + 7 (812) 325 84 00
моб: + 7 911 929 60 04

e-mail: Mikhail.Usachev@polikom.ru

ПОЛИКОМ про