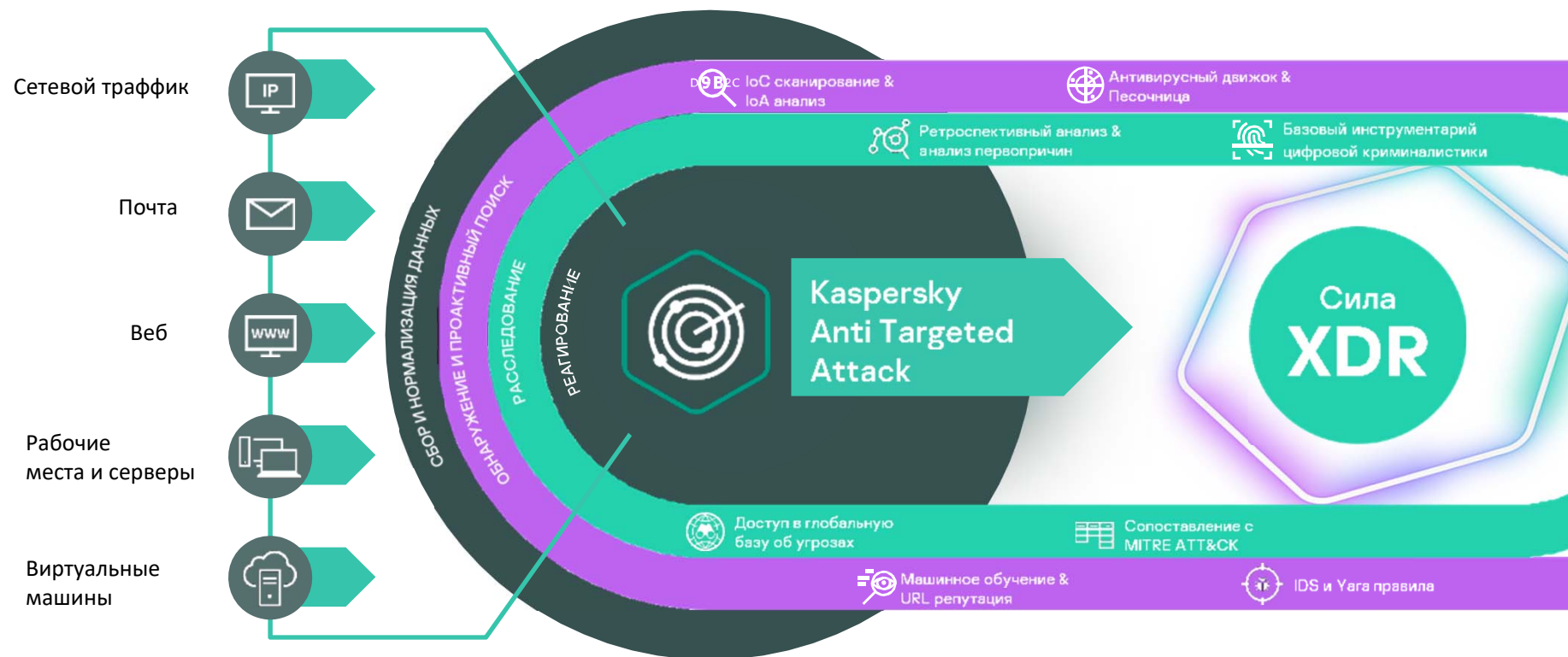


Kaspersky Anti Targeted Attack



ПОЛИКОМ про

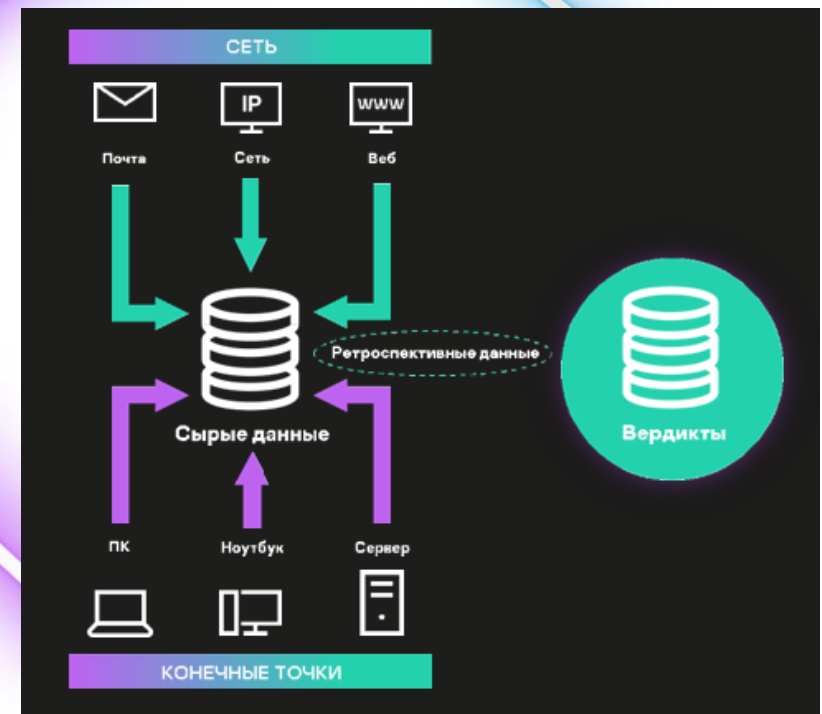
Платформа KATA с EDR: Расширенные возможности защиты XDR



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 проведении 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



Обнаружение угроз и информирование об угрозах

Обнаружение

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

Сканирование инфраструктуры на наличие
индикаторов компрометации

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

Передовая песочница

Рекомендации по расследованию и реагированию

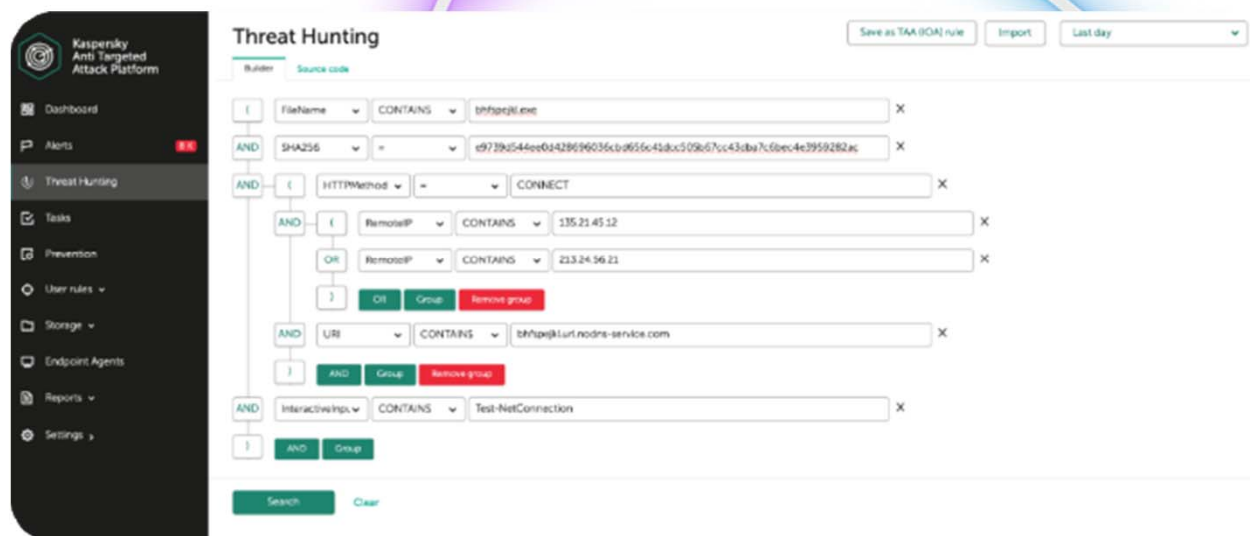


IP	Created	Released	Details	Source	Destination	Technology	Status
193.54.22.47	36/04/2018	Released	Domain: bug-jarvis.com	193.54.22.47	193.54.22.47	High	New
193.54.22.48	36/04/2018	Released	Domain: 193.54.22.48	193.54.22.48	193.54.22.48	High	New
193.54.22.49	36/04/2018	Released	Domain: 193.54.22.49	193.54.22.49	193.54.22.49	High	New
193.54.22.50	36/04/2018	Released	Domain: 193.54.22.50	193.54.22.50	193.54.22.50	High	New
193.54.22.51	36/04/2018	Released	Domain: 193.54.22.51	193.54.22.51	193.54.22.51	High	New
193.54.22.52	36/04/2018	Released	Domain: 193.54.22.52	193.54.22.52	193.54.22.52	High	New
193.54.22.53	36/04/2018	Released	Domain: 193.54.22.53	193.54.22.53	193.54.22.53	High	New
193.54.22.54	36/04/2018	Released	Domain: 193.54.22.54	193.54.22.54	193.54.22.54	High	New
193.54.22.55	36/04/2018	Released	Domain: 193.54.22.55	193.54.22.55	193.54.22.55	High	New
193.54.22.56	36/04/2018	Released	Domain: 193.54.22.56	193.54.22.56	193.54.22.56	High	New
193.54.22.57	36/04/2018	Released	Domain: 193.54.22.57	193.54.22.57	193.54.22.57	High	New
193.54.22.58	36/04/2018	Released	Domain: 193.54.22.58	193.54.22.58	193.54.22.58	High	New
193.54.22.59	36/04/2018	Released	Domain: 193.54.22.59	193.54.22.59	193.54.22.59	High	New
193.54.22.60	36/04/2018	Released	Domain: 193.54.22.60	193.54.22.60	193.54.22.60	High	New
193.54.22.61	36/04/2018	Released	Domain: 193.54.22.61	193.54.22.61	193.54.22.61	High	New
193.54.22.62	36/04/2018	Released	Domain: 193.54.22.62	193.54.22.62	193.54.22.62	High	New
193.54.22.63	36/04/2018	Released	Domain: 193.54.22.63	193.54.22.63	193.54.22.63	High	New

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

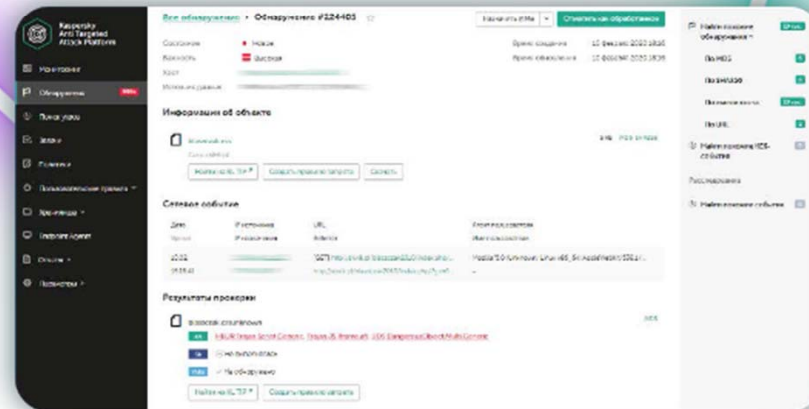
Поиск по техникам MITRE ATT&CK

Учитывать в поиске особенностей и специфике защищаемой инфраструктуры

Детальное расследование инцидентов

Расследование

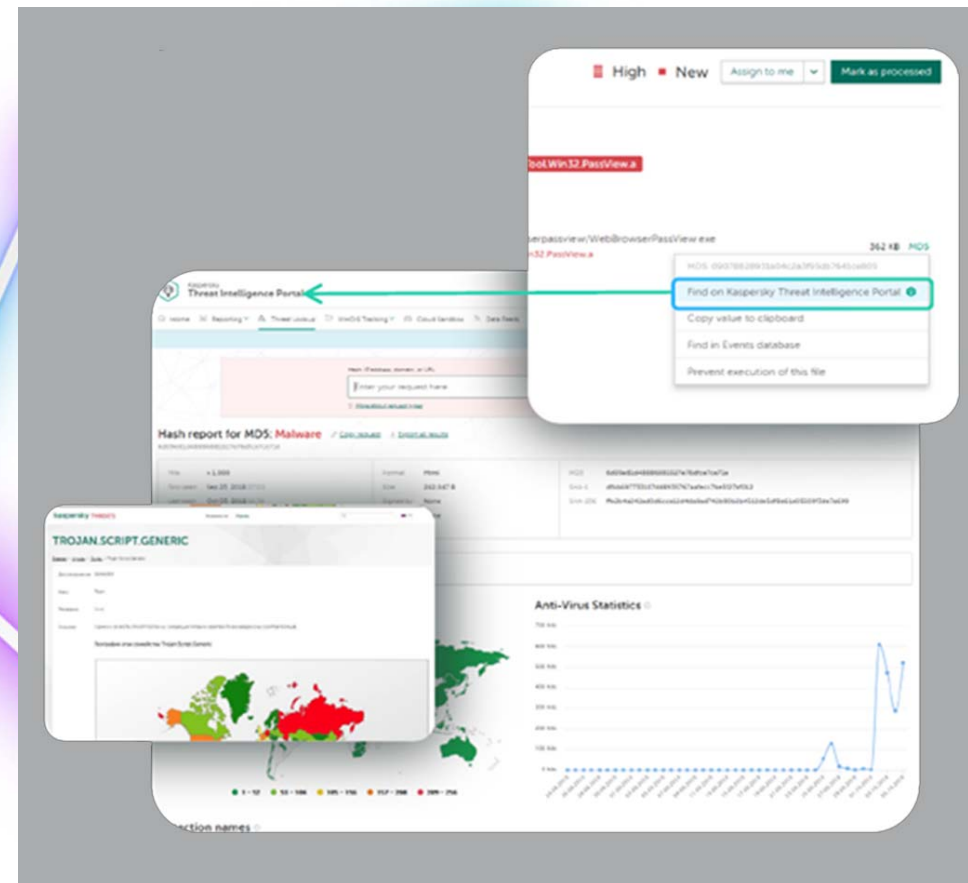
- Расширенные возможности анализа первопричин
- Рекомендации по расследованию
- Работа с порталом Kaspersky Threat Intelligence
- Сопоставление событий с глобальной базой знаний тактик и техник MITRE ATT&CK
- Обогащение подозрительных событий понятным описанием, трактовкой, примерами и рекомендациями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



Взаимодействие с глобальной аналитикой киберугроз

Обогащение

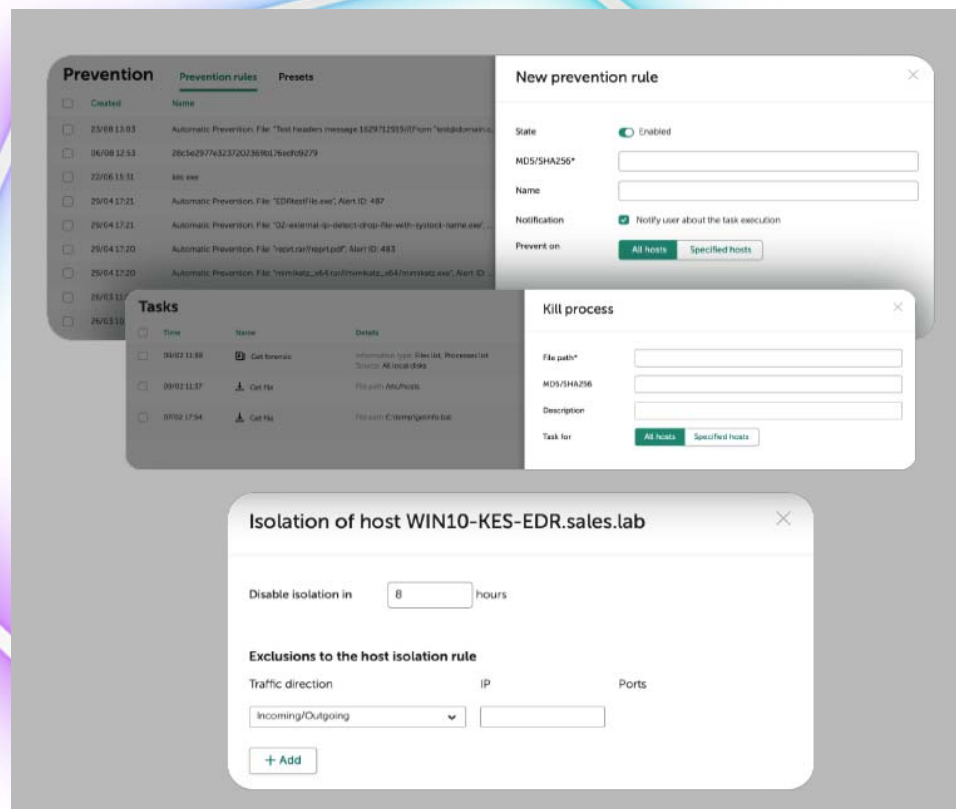
- Встроенный доступ к Kaspersky Threats
- Обогащение данными с матрицы MITRE ATT&CK
- Доступ на портал Kaspersky Threats Lookup
- Проведение запросов по угрозам вручную по базе данных
- Получение дополнительных данных для проактивного поиска угроз и проведения детального расследования инцидентов
- Непосредственный 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



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

The logo consists of a black rectangular box with the word "kaspersky" in white lowercase letters at the top, a thin teal horizontal line below it, and the words "Platinum Partner" in white uppercase letters below the line. The background of the slide features a white and grey geometric pattern of overlapping polygons.

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 The logo for "ПОЛИКОМ" is in a bold, grey, sans-serif font. To its right is a small blue square containing the word "про" in white lowercase letters.