

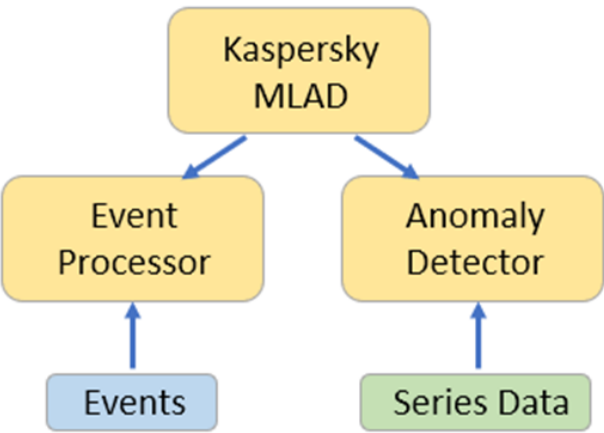
Kaspersky MLAD: ?????? Event Processor (EP)

1. ?????????? ???????????

????? ???????? ?????????????????? ?? ?????? ?????????????? ? ?????????????? ?????? ?????????? ????????
????????????????? ?????????? Kaspersky MLAD ? ??? ?????????? ??????????????????. ??? ??? ?????? ?????????? ??
????????????? ?????????? ?????????? ?????????????? ???????? ? ???????? ?????? ? ?????????????? ???????? ???
????????? ?????????????? ??????.

2. Kaspersky MLAD - ????? ?????????? ????????

??? ?????????????? ?? ????, ?????? ??? ?????????????? ??? ?????????????? ?? ?????????????? ???
????????????? ???????? ? Kaspersky MLAD, ? ?????? ? ??????, ?????????? ?????????????????? ???????? ? ??????
????????????????????? ?????????? ???????? ?????????? ????????

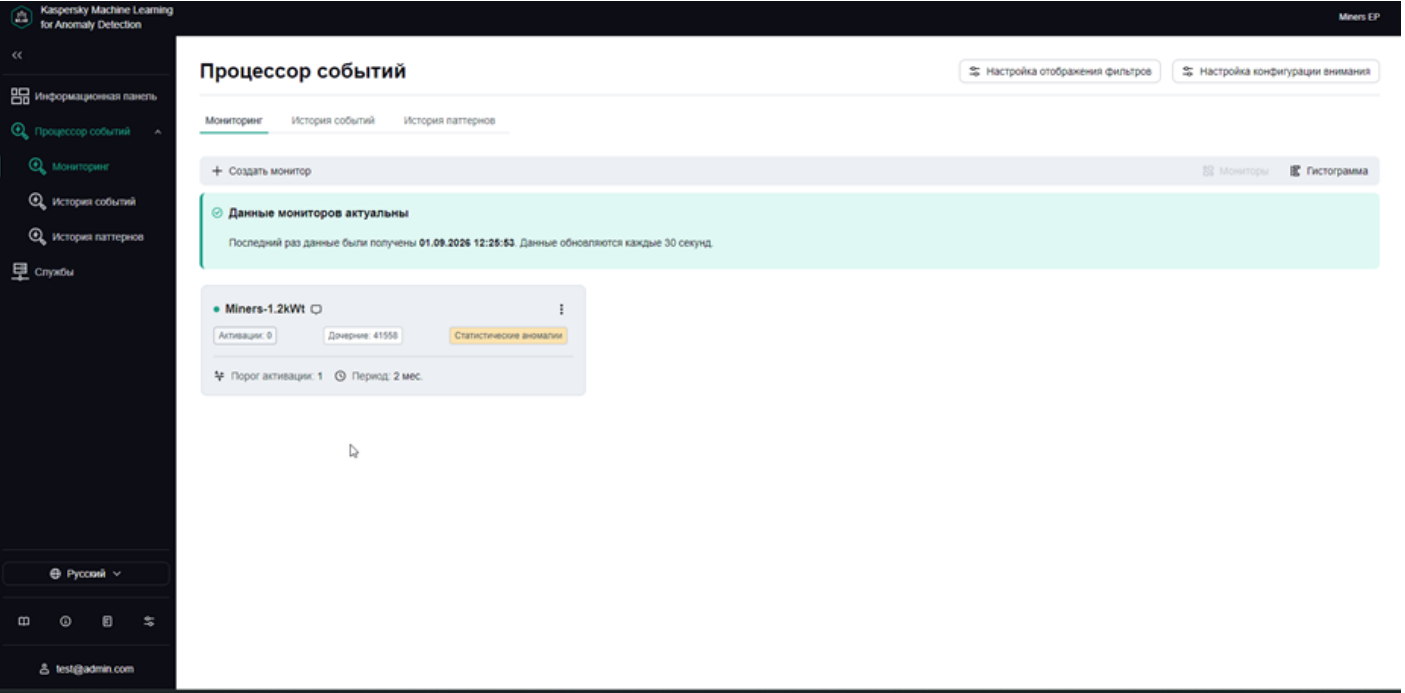


??-??????, ??? ?????????????? ???????? ?? ?????????????????? ?????????????????? (????????????? ??????). ?? ????, ????
????? ? ?????????? ?????????????? ?????????????????????? ??????????????, ?????????? ?????????????? ???????? ??????????????????
?????????????, ??????????, ??????????????????, ??????????, ??????????, ???????? ? ?????????. ? ???????? ? ???????? ??????????
????????????? ???????? ?????????????? ?????????????? Kaspersky MLAD, ?????????? ?????????????? ?????????? ? ??????????????
?????????????. ??? ?????? ??? ? ? ?????????????? ?????? ?? ?????????????? ?????????????? – ???????? ?????????????? ??????????
??????? ?????????????????? ???????? ? ?????????????????? ?????????????? (????????????, ??? ?????????????? ??? ??????????????????????
?????????).

?? ? ?????? ???????, ?????? ??? ? ??? ? ???????? ??? «?????? ?????????» - «????????????».

??? ?????? ??? ?????????????? ?????????????? ?????????????? ?? ?? ?????????????? ??????, ?? ? ???????? ?????????? ?? ???????? ???
????????????????? ?????????????????? ?????????????, ?? POS-?????????????????, ??????????????????, ?????????????????????? ??????????????????????,
????????? SIEM ? ??? ??????. ??????????, ??? ? ???????? ???????? ?? ?????? ?????? ??? ? ???????? ?????? ??????, ?
????????? ? ?????????????????? ??????????. ?????? ???????? ???????? ?????? ?????????? ?????? ?????????????? (? ????????
?????????) ?????????????? ?????????????????????? ?????????????? ? ??????????. ??????????, ?????????? ?? POS-?????????????
??????? ?????????????? ?????????????????????? ??????????, ID ??????????????, ?????? ??????????????, ?????????????? ??????????,
????????????????????????? ?????????????? ? ?.

??? ?????? ? ???????????? ???????? ? ?????????????????????????????????? ???????? ? Kaspersky MLAD ????? ??????????
????????, ????????? ?????????????? ?????????????? ?????????? (Event Processor). ???????? ???????? ???????? ? ????????
????????? ??????????, ?? ??? ??? ???????? ?????????????? ?????????????? ?????????????.



3. ?????????? ???????? ???????? EP

??? ????? ?????????? ?????, ?????????? ?????????????????????? ?????????????? ?????????? ?????????? ???????? ? ??????????????
????????? ? ?????????????????????????????? ??????????.

?????????, ??? ??? ???????? ? ?????? ???????, ?????????? ?????????? ?????????? ?????????? ???????? ?????? ?
?????????????, ?? ?????????? ?????????????????? ?????????????? ?????, ?????????? ?????????????????? ? ???????? ?????????????
?????????. ?????????? ? ?????????????????? ?????????? ?????????????????? ???????? ??? ??????????????, ?????????? ??????????????
????????????????????????????? ?????, ? ?????? ?????????????????? ???????? ?????????????????????????? ??????????. ??? ?? ???????? ??
????????????? ?????????????????????? ?????????? ??? ??????????, ???????, ?????? ?????????? POS-????????????????? ??
????????? ?????? ? ??????????. ?????????? ?????????????? «?? ??????».

?? ???????? ?????????? ? ?????????????? ?????????????? ? ?????????????? ?????????? ? ?????????????? ?????????? ?????????????? ???
????????????????? ?????????????? ??????????. ??? ?????????????????????? ?????????????? ?????????? ?? ?????????????? ??????????. ?????????????? ??????
??? ?????????????? ? ?????????? ??????????

События

Позволяет отслеживать появление отдельных событий, например, событий с новыми значениями определенных параметров.

Значения параметров

Позволяет отслеживать появление определенных значений в параметрах событий, например, новых значений по определенному параметру события.

Эксfiltrация данных по DNS

Позволяет отслеживать DNS-запросы, содержащие признаки эксfiltrации данных.

Часы активности

Позволяет отслеживать необычную активность по времени событий в фокусе внимания.

Паттерны

Позволяет отслеживать закономерности в поведении объекта в фокусе внимания.

События головы внимания

Позволяет отслеживать события в фокусе внимания.

Статистические аномалии

Позволяет отслеживать аномалии путем статистического анализа событий.

Уникальные обобщенные

Позволяет отслеживать уникальные события или паттерны объектов в фокусе внимания.

Похожие обобщенные

Позволяет отслеживать общности в поведении объектов в фокусе внимания.

????????????, ??? ? ??? ????? ????? ????????? ? ????????? ?????????????? ? ??????, ? ?? ????? ?????????
???? ?????????????? ? ?????? ? ?????????? ??? ??? ?????.

???? ?? ?? ????? ????????? ?????????? ? SIEM ??? ?????? ??? ??????, ??? ?? ?????????????? ???-??
???????? ? ????????? ????????? ?????? ????? ?????????????? ?????? ?? ?????? ?????????????? ? ??????
??? ????????????? ?????? ? ??? ??????. ??? ?????????? ?????????????? ?????????? ?????? ?
????????, ?????? ?????? ?????????? ?????? ?????????, ??? ?????? ?????????.

? EP ??? ?????? ????????? ?????? (????? ?????????? ?????????? ??? ?????????? ??????)
????????? ????????? ???????.

События

Позволяет отслеживать появление отдельных событий, например, событий с новыми значениями определенных параметров.

?? ?????? ?????????? ??? ?????? ?????????? ?????????? ?????????? ?? ?????? ?????????????????? ?????
????????? ?? ?????????????????? ??? ???????.

Параметры активации

Порог активации

1

Тип активации

☒ Отслеживать только новые элементы

Фильтры

+ Добавить фильтр

☐ Отслеживать по всем значениям одновременно

Параметр события

Тип фильтра

Тип значения

UserHost

Параметр

Новые значения

?????? ?????? ???, ?????? ? ??? ?????? ?????????? ?????? ?????? ? ?????? ??? ??? ?????????? ???
UserHost, ?? ?????? ?????????? ?????????????? ?????????.

??? ????, ?????????? ?????? ? ?????????? ?????????? ?????????? ?????????? ?????????? ?????????? ?
????????????? ?????????? ?????????.

????????????, ?????? ??? ?????? ?????? ?????????? ?????????? ?????????? ?? ????????? ? ??????
????????? ????. ??? ?????????, ?????? ?? ?????? ?????????? ?????????? ?????????????? ?????? ?????????
??????? ? ?????????? ??? ??? ?????.

??? ??????? ?????????? ?????? ?????? ?????????????? ??? ??? ?????????:

Часы активности

Позволяет отслеживать необычную активность по времени событий в фокусе внимания.

??? ?????? ?????????? ?????????? (? ?????????????? ??????) ?????? ?????????? ?????????????????? ??
????????????????? ?????????? ???????, ?????????? ?? ?????????? ??????, ? ?????? ?????? ?? ??????????

??? ????? ? EP ?????????? ?????????????????? ?????????, ??????? ?????????????? ??????? ??????????. ???
 ?????????? ??????? ????????? ?????????, ?? ????????? ?????? ?????????????????? ?????????, ? ????????? ??
 ??????????? ?????????????? ?????????.

?? ????????? ???? ?? ??????? ?????? ?????? ?????????, ??????? ?????????????? ?? IP ?????? ?????? ?
 ?????????? ????????? ?? ?????????? ????????? ?????????? ?????????? ?? ???? ? ?????????? ??????????????????
 ?????????????? ????????? ?? ?? ?????????? |P ?????? ???? ?????????????.

Параметры активации

Голова: **внимание**

АТН: **Node**

Порог аномальности: **0**

☐ Отслеживать необычную активность по часам дня недели

??????? ????? ?????????? (? ?????????????? ????? ??? ??????????, ?????????????? ?????????????? ??????? ?? DNS) ?????????? ?????????????????? ? ?????? ????? ?????????????????? ??? ?????????? ?????????????? ?????????? ??????.

? ??????, ??????, ?????????? ?????????????? ??????? ???? ???? ??????????? ?? ??????????
 ????????? ? ????????????????? ???.

События

Позволяет отслеживать появление отдельных событий, например, событий с новыми значениями определенных параметров.

Значения параметров

Позволяет отслеживать появление определенных значений в параметрах событий, например, новых значений по определенному параметру события.

Эксfiltrация данных по DNS

Позволяет отслеживать DNS-запросы, содержащие признаки эксfiltrации данных.

Часы активности

Позволяет отслеживать необычную активность по времени событий в фокусе внимания.

Паттерны

Позволяет отслеживать закономерности в поведении объекта в фокусе внимания.

События головы внимания

Позволяет отслеживать события в фокусе внимания.

Статистические аномалии

Позволяет отслеживать аномалии путем статистического анализа событий.

Уникальные обобщенные

Позволяет отслеживать уникальные события или паттерны объектов в фокусе внимания.

Похожие обобщенные

Позволяет отслеживать общности в поведении объектов в фокусе внимания.

??? ????? ?? ?????? ?????? ????????, ?????? ?????????????? ?? ?????????????? ? ?????? ?????? ?? ?? ?????????????????????.

Голова внимания ATN_Miners

×

Имя

ATN_Miners

Состояние

Активна

Распознавание паттернов

Выключено

Обобщение параметров условий

Выключено

Предмет внимания

Имя параметра

Consumer

Тип внимания

Внимание

Тип значения

Все значения

Значение

Все значения

Условия

Параметр события	Тип условия	Тип значения	Значение
Power	Параметр	Все значения	

? ?????? ??????? ??????? ??? ?????????? ?????????????????? ????????? ? ?????????????????? ?????? ?????? ??????????

Тип активации
☐ Отслеживать все элементы

Фильтры

+ Добавить фильтр

Голова внимания

ATN_Miners

Метод расчета отклонений

По отношениям верхней и нижней дисперсий к среднему

Тип статистического интервала

Последний интервал

Вложенный шаг (сек.)

87600

Смещение вложенного шага (сек.)

87600

Метод сравнения

Отношения верхней и нижней дисперсий к среднему за вложенный шаг больше соответствующих верхнего и нижнего порогов

Сравнение среднего со значением порога

Не используется

Параметр события для анализа

☐ Использовать интегральное по времени среднее

Порог отношения верхней дисперсии к среднему на вложенном шаге

0

Порог отношения нижней дисперсии к среднему на вложенном шаге

0

????? ?????????? ?????????? ??????????, ??? ?? ??? ???? ???? ?????????? ?????????????? ?????? ?????????????? ?? ??
????????? ?? ???? ?????? ?????? ?????????????????, ? ?? ?????? ?????????? ?????????? ?????????????????? ??????????
? ?????????????? ?? ?? ?????????? ?? ???.

4. ?????????????

????????????? ?????????????? ?????????? ?????????????? ?????? ?????????????? ??????, ?????????? ?????? ??????????????????
?????????. ?????????????? ?????????????? ?????????? ? ?????? ?????????????? ?? ?????????????????? ?? ??????????????
????????????????? ?????????? ??????, ??? ??? ??? ?????? ?????????????????????? ? ?????????????? ?????? ??????????????. ?
????????????????? ?????????????? ?????????????? ?????????? ?????? ?????????????????, ? ??? ?????? ??? ?????????????? ?????????????.