

Kaspersky MLAD: ?????????? ? KUMA ?? Syslog

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

?????? ?????????? ?????????? ?????????? ?????????? Kaspersky MLAD ??? ?????????? ? KUMA ?? ?????????? Syslog.

???? ?????? ????????????? – ?????????? ?????????? ?????????? ?????????????? ?? Kaspersky MLAD ? SIEM ?????????? ?? ?????????????? ?? ?????????????????? ?????????????? ? ?????????????????? ??????????.

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

[image.png](#)

2. ?????????????? ????????

?????? ?????? ?????????????? ??????????? CEF-?????????? ? ??????? Kaspersky MLAD ?? ?????????? ?????????? ?????????????????? ? SIEM-?????????.

??? ?????? ?????????????? ? ???? ??????????????????, ?????? ? ??????????? ???????????, ?????? ? ??????????? CEF-?????????????.

????? ??? ?????????????? ?????????????????? ?????????????????? ?????????????? ?????????? ?????????? ?????????????????? ?????????????????? ?? Syslog-????????, ?????????? ??? ?????????????? (TCP ??? UDP), ?????????? ?????? ? ????? Syslog -?????????. ????? ?? ?????????????? ?????????????????? ?????????????? TLS-?????????????, ?? ??? ?????????????? ?????? ?????????????? ?????????????/????????????? ????? ?????????? ? CA-????????????????? ??? ?????????????????? ?????????????? ??????????.

[image.png](#)

?????? ?????? ?????????????? ? ?????????? ??????, ?????? ? ?????????, ?????? ? ????????? ??????????????. ??????????? ????????? CEF connector, ??? ?????????????????? ??, ????? ?? ?????????? ?????????????? ? ??????????????.

[image.png](#)

?? ?????? ?????????????? ?? ?????????? MLAD ??????????????.

? KUMA ?????????????? ? ?????????? ??????????, ?????? ??????????????????.

[image.png](#)

? ?????????? ??????????? KUMA ?????????? ?????????????????????? ?????????????????? ?????????????? [OOTB] Syslog CEF. ?????????????? ?????? ?? ?????????? ?????????? ?????????????????? ? ?????????????? ? ??? ??????????????.

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

[image.png](#)

?????????? ??? ??????????????, ?????????????? ? ?????, ?? ?????????? KUMA ?????? ?????????????? ?????????????????? ?? Syslog. ??????????????, ??? ?????????????? ?????????????????? ? MLAD ?????????????? ? ?????????????????? ? ?????????? ??????????.

????????? ?????????? ???????? ?? ?????? ?? ?????? ?????????? Syslog. ?? ???????? ?????????? ?????????? ??
??????? ??????????, ?? ?????? ?????????? ???????? Syslog, ???????????? ?? MLAD. ??? ?????? ??
????????????????? ?????????? ???????? ?????????????????? ??????. ???????? ?????????? ? ?????????? ????????
??????? ? ?????????????? ?? KUMA, ? ? ?????? ?????????? ?? ??????????????,
????? ?????????? ?????????? ??? ???????? ?????? ?????????? ?????? ????????
????????????????? ??????.

[image.png](#)

??? ?????? ???????????? ?????????? ?????????????? ???????? (????? sudo) ?? ?????? ? KUMA.

[image.png](#)

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

[image.png](#)

????????? ? ?????? ?????????? ???????? ? ??????????, ?? ??? ?????? ?????????? Syslog
????????.

[image.png](#)

????????? ? MLAD ? ???????????? ?????-????? ?????????? ?????????, ?????????, ???????? ? ??????
???????? ? ???????.

????? ?????????? ???? ?????????? ?????? ? KUMA ? ???????? ?????? ????????? ? ?????????.

[image.png](#)

C????????? ?????????? SQL-?????. ?? ???????? ? ?????? ???????? ?????????????? ?? MLAD.

[image.png](#)

Revision #3

Created 10 April 2026 13:57:30 by Эльдар Юсуфов

Updated 23 October 2026 11:20:47 by Эльдар Юсуфов