Путь новичка в KUMA

????? ?????????? ? ???? ?????? KUMA SIEM. ??? ???????? ???????? ??? ?? ?????????? ? ???????? ?? ?????? ??????? — ???????????????, ??? ?? ?????.

Путь изучения □□➡□□➡□□

1. □□ Что такое SIEM и архитектура KUMA

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

- ??? ????? SIEM ? ????????? ?????? ????????
- ? ??????? Kaspersky Unified Monitoring and Analysis Platform (KUMA)
- ??????????? KUMA
- ????? ???????? ????????????? ??????????? KUMA
- ?????? ????????????? KUMA

---

2. ⚙ Подготовка инфраструктуры

??????????? ????????????? ??? ????????? ????????????? KUMA

- ?????????? ????????????? ??? ????????????? KUMA
- ????????? ??????

> ?? ????????? ??????? ???????? ????? ??????????? ????????? ? ?????? ????????????? ???????? ? ????????????? ?????????? ??????????? KUMA.

---

3. □□ Установка и базовая настройка KUMA

?????????? KUMA ? ????????? ????????????? ???? ?? ?????????

- ????????? KUMA
- ??????? ????????? KUMA
- *(???????????)* ?????????? KUMA ? ?????? ???????? ?????????

---

4. □□ Нормализация, модель данных и хранение событий

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

- ??? ????? ????????????
- ?????? ?????? ?????????????????? ???????
- ????????????? ????????? ???????
- ???????? ???????? ? KUMA
- ???? ???????? ?????? ? KUMA
- ? ???????? ClickHouse ? ??????? ?????????

---

5. □□ Подключение источников событий

Подключение источников событий — ??? ???????? ??????? ??? ??????????? ???????????? ? ??????????? ??-??????????????. KUMA ????????, ??????????? ? ??????????? ?????? ?? ????????? ?????????? ??? ????????? ????????, ????????????? ???????? ? ????????????? ????.

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

- ??????? ??????????: ??????????????, ???????????, ?????????? ?????? (????????, Cisco ASA, Palo Alto).
- ??????? ???????/??????? ??? ??????????? ?? Windows ? Linux.
- ???????????????? ???????: Active Directory, DNS, DHCP, ???????? ???????.
- ??????????: ???-??????? (????????, Apache, IIS), ???? ?????? (????????, MySQL, MSSQL).
- ??????? ????????????: ??????????, IDS/IPS (??????? ??????????? ? ????????????? ?????????), VPN ? ??????.
- ???????? ???????.
- ?????????? IoT.
- ? ??????.

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

- Windows (????? ?? ????????? ????????)
  - ????????? ????????? ??????? Windows ? ??????? Kaspersky Endpoint Security
  - ????????? ????????? ??????? Windows ? ??????? ?????? KUMA (WEC)
  - ????????? ????????? ??????? Windows ? ??????? ?????? KUMA (WMI)
- Linux
  - ????????? auditd ? Unix-????????
  - ???? ??????? auditd ? ??????? Rsyslog

    - ???? ??????? auditd ? ??????? Syslog-ng
- ???????? ??????????? ???????????
- ???????? Microsoft
- NGFW ? ?????? ??????? ????????????
- 1?, ???-???????, ????????????? ? ?????? ???? ?????????
- C????? ??????-??????? "????????? ?????????? ???????"

---

6. □□ Работа с событиями

??????? ?????????? ? ??????????, ??? ? ???? ?????????

- ?????? ? ?????????
- ???????? ???????? ?? ????????

---

7. □□□ Интеграции

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

- ?????????? ? Kaspersky Security Center
- ?????????? ? Active Directory
- ?????????? ? Kaspersky CyberTrace
- ?????????? ? Kaspersky Threat Intelligence Portal

---

8. □□ Правила корреляции и детектирование

????????? ??????? ??????? — ?????? ?????? ???????? ??? ????????? ?????? ???????.

- ??? ????? ???????????? ??????? ??? KUMA
- Community Pack — ??????? ??????? ?????????? KUMA (?????? ??? ???????: `q123123Q!q123123Q!` ??? `q123123Q!KLaapt-M4`)
- ?????? ???????? ??????? MITRE ATT&CK ????????? ?????????? KUMA
- MITRE ATT&CK ? SOC — ??? ????????????
- ??????? ???????? MITRE ATT&CK ????????? "???????????? ????????????"

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

- ???? ?????? ??????????
- Cookbook: ?????? ? ????????? ??????????

---

9. □□ Работа с алертами и инцидентами

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

- ?????? ? ????????
- ??????????? ?? ?????? ? ?????????
- ???????? ??????? ?????????? ?? ???????????
- ???????? ???????? ?????? с ??????????? ? KUMA
- ?????????????? ????????

---

10. □□ Мониторинг и отчетность

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

- ?????? ???????????
- ??????

---

11. □□ Сервисы ИИ

«??? ????? ???? ??????, ??????? ? ~~????????~~ ??????» (c)

- ???????? ???????? ??
- KIRA
- ??????? ???????
- ????????? ???? DLL Hijacking

---

12. □□□ Эксплуатация KUMA

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

- ??????????? ????????? ?????????? ???????
- ????????? ??????????? ? ????????????? ???? KUMA
- ?????? ????????????? ?????? SIEM

---

13. ⚠ Что-то не работает

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

- FAQ

- ??????????
- TG ??????????

---

14. □□ Видеоматериалы

????????? ????? ?? KUMA:

- ????? KUMA
- Rutube
- Youtube
- ?????? ? ???????????????
- ?????? ? ????????? ??????????

??? ??????:

- KUMA 4.2
- KUMA 4.0

KUMA Community Meetup

- ?????????? ??????????
- ????? ????????????
- ????? ????????????

---

15. ✍ PoC Чек-лист

? ???? ?????, ??? ????? ???????????????

Чек-лист

- ☐ ?????????? ?????
- ☐ ????????? KUMA
- ☐ ??????? ?????????
- ☐ ?????????? ??????????
  - ☐ ????????? ????????? ??????? Windows
  - ☐ ????????? ????????? ??????? Linux (Auditd)
  - ☐ ????????? ????????? ??????? Kaspersky Security Center

- [ ] ?????? ? ?????????
- [ ] ??????????
  - [ ] ?????????? ? Kaspersky Security Center
  - [ ] ?????????? ? Active Directory
  - [ ] ?????????? ? Kaspersky CyberTrace
  - [ ] ?????????? ? Kaspersky Threat Intelligence Portal
- [ ] ??????? ??????????
- [ ] ?????? ? ????????
- [ ] ??????????? ?? ?????? ? ?????????
- [ ] ???????????????? ????????
- [ ] ?????? ???????????
- [ ] ??????
- [ ] ??????? ??
  - [ ] KIRA
  - [ ] ??????? ???????
  - [ ] ????????? ???? DLL Hijacking
- [ ] ????????? ?????????? ???????
- [ ] ????????? ??????????? ???? KUMA

16. □□ Полезные ресурсы

- ???????? ?????? ?? ??
- Community-??????? (GitHub)
- ????????????? ??????? ? ????????? ?? GitHub ???????????? KUMA Community
- ????????????? ????? ????????????? ??????????

Revision #72
Created 2026-06-09 09:19:47 UTC by Dmitry Borisov
Updated 2026-08-18 15:13:18 UTC by Dmitry Borisov