Общая информация

- ????????????? ?????????
- KATA ? ?????????????? ??????????? (PCN/SCN): ??????? ?????? ? ????????????????? ???????????
- Cheat Sheet ?? ??????????? KATA c KUMA

Маркетинговые материалы

Данный раздел содержит ссылки на маркетинговые материалы по продукту KATA&KEDR&NDR. Все материалы представлены в виде ссылок для скачивания.

Основные материалы:

- ???????? ????? KATAP - ??????
- ???????? ????? KEDR - ??????
- Datasheet KATA – ??????
- Datasheet KEDR – ??????
- ???????? Why KATA? – ??????
- ???????? ??? ??????? ?? ????????? KATA – ??????
- ???????? ??? ??????? ?? ????????? KATA/KEDR – ??????
- ???????? How to sell – ??????
- What’s new KATA&KEDR – ??????

Видеоролики:

- ????????? ????? ?? Kaspersky Anti Targeted Attack Platform - ??????

Истории успеха/Россия и СНГ:

- ?????? – ??????
- ??-???????????? – ??????
- Head Hunter – ??????
- ??????? – ??????
- ?????? – ??????
- ??? – ??????
- ????????????? ?????????? ??????? – ??????
- ??????????? ??????????? ???????????? ???????? – ??????
- ??????????? ???? – ??????
- KICB – ??????
- ?????????-? – ??????
- ???????? ????????????? ??????? – ??????
- ????????? ?????????? – ??????
- ??? ??????? – ??????
- ?????? ???? – ??????

Материалы по запросу:

?????????????? ????????? ?? ?????? ????????? ????? ????? ? ??????? pre-sale ?????????
AntiAPT.

KATA в распределённой инсталляции (PCN/SCN): принцип работы и эксплуатационные особенности

> **Примечание.** ???????? ??????????? ??? AntiAPT Community ? ???????????? ??? ????????????? ????????? ????????? ??????. ?? ?? ???????? ??????????? ???????????? ???????.

????????????? ??????????? Kaspersky Anti Targeted Attack Platform (KATA) ???????????, ????? ????????? ?????? ?????? ?????????? ??? ?????????? ????????/????????????? ?/??? ?????????????? ?? ?????????? ??????? ? ?????? ????????????? ??????.

Содержание

1. ?????????? ? ???????? ??????????
2. ??????? ? ???? (PCN/SCN)
3. ??? ????????????? ?????????? ? ??????
4. ?????? ??????: ?????? ? Threat Hunting
5. ???????????, ????? ? ??????
6. ????????? ? ?????????????
7. ??????????? SCN ? PCN: ??????? ? ???????????
8. ????????? ???????????: ?????? ???????????
9. ????????? ? ????????? ???? SCN

1. Назначение и сценарии применения

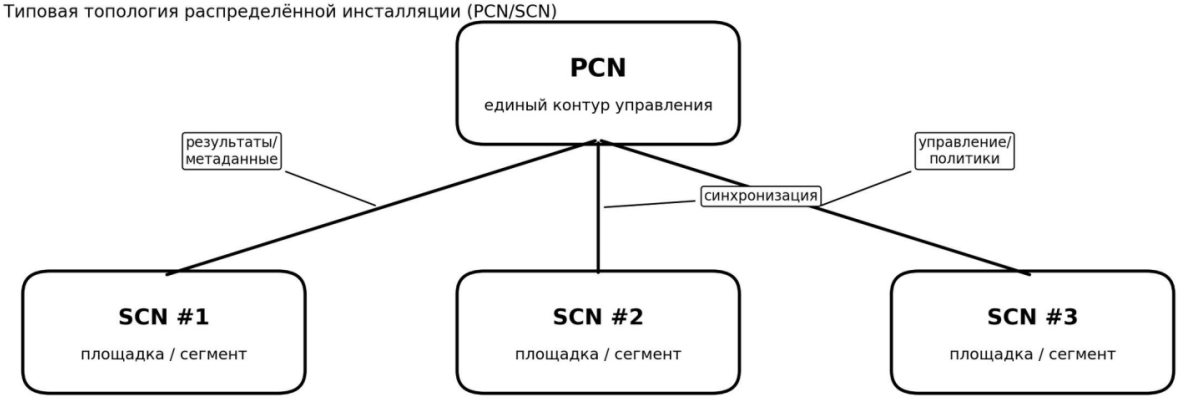
? ????????????? ??????????? ????????? ???????? Central Node ???????? ??? ?????? ???????: ????????? ?????????????, ? ????????? ?????? ??????????? ????? ? ????????? ??????? (?? ?????????/?????????/????????).

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

2. Термины и роли (PCN/SCN)

- **PCN (Primary Central Node)** — ??????? ?????? ??????????. ?????? ???????? « ?????? ??????» ?? ???? ???????????? ?????????.
- **SCN (Secondary Central Node)** — ??????????? ??????. ??? ???????, ??????????? « ?????????» ???????? ? ?????????????? ?????????? ? PCN.
- **Тенант** — ?????????? ??????? (???????????/??????), ??? ??????? ??????? ?????????? ?????? ?????? ? ?????????? (? ?????? ????????????????).

Схема 1. Типовая топология распределённой инсталляции (PCN/SCN)



3. Как распределяются управление и данные

? ?????????????? ??????????? PCN ????????? ???? ??????????? ????? ??????????, ? SCN — ???? ??????????? ?????. ??? ???? ????? ???????? ? ???????? ??????????????, ?? ??????????? ??????? «?????? ????????????? ???, ??? ??????».

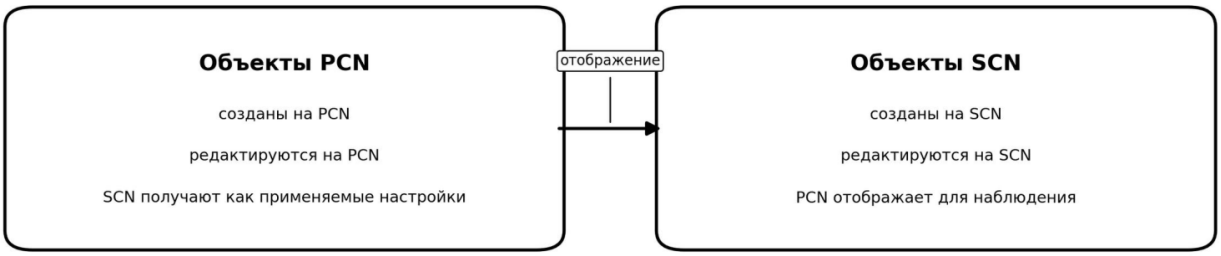
3.1. Что обычно централизуется на PCN

?? ???????? ?? PCN ??????? ????? ?????? ????????, ?????? ? ???????, ? ????? ????????????? ?????? ? ?????????? ????????????? ?? ???? ???????????. PCN ????????? «????????» ?? ?????? , ??????? ????????? ?? SCN.

3.2. Принцип «создано здесь — редактируется здесь»

? ???????????? ????? ??????? ???????????? ? ???????? ????????????????: ???? ?????? ?????? ?? PCN, ??? ????????? ???? ???????????? ?? PCN; ???? ?????? ?????? ?? SCN — ????????? ???????????? ?? ?????????????? SCN. ??? ??????? ???? ?????????? ? ???????? ?????????????? ????? ?????????/??????????.

Схема 2. Принцип «создано здесь — редактируется здесь»



4. Потоки данных: алерты и Threat Hunting

SCN ????????? ???? ? ????????? ?????? ? ?????? ????? ????????. ?????????? (???????/??????????/???????/??????????) ???????????? ??? ???????????? ????? ??????? ?? PCN.

- **Алерты** ???????????? ?? ?????? PCN ??? ???????????????? ???????? ? triage.
- **Threat Hunting** ? ?????????????? ?????????? ??????? ???????????? ??? «?????? ?????» ?? ?????????: ?????? ???????????? ?? ???????????? ??????????, ? ?????????? ?????????? ?? ???????????? ?????.

5. Пользователи, права и сессии

??? ???????????????? ?????? ????? ????????? ????: ?????????? ????????????? (PCN) ? ?????????? ????????? (SCN). ? ??????? ???????? ??????? ?????? ? ???? ???????????????? ????????????????, ? ?????? ? ?????????? ????????? ????????????? ???????.

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

6. Хранилище и лицензирование

? ????????????? ?????????? ?????????? ??????? ??????? ??????? ??????? ????????? ? ????????????? ?? ?????????? ?????: ???? ??? ???????????????? ?????????? ?????? ?????? ? ???????? ??????? ?? ????, ????? ????????? ?????????? ?? ?????????? SCN.

????????: ?? ????? ????????????? ??????? ??????????, ????? ???? ?????? ???????? ? ??? ????? (retention), ???????? ??? ???????????? ?????? ? ????????.

7. Подключение SCN к PCN: доверие и верификация

?????????? SCN ? PCN — ??? ???????????? ?????????? ?????? ??????????. ? ??????? ???????? ???????????? ??? ?????????? (????????, ????????? ????????? ???????????), ??????? ????????? ????????? ?????????? ? «?? ????» ???????????? ????.

> **Важно.** ????????????? ??????? ?????????? ?????????: ??? ??????? ??????? ?????? ??? ?????????? SCN, ??? ????????? ?????? ????????? ?????????? (??? ??????), ? ??? ?????????? ???????????? ?????????? ????????.

8. Резервное копирование: важные ограничения

??? ????????????? ?????????? ??????? ???????? ??????? ????????? ?????????? ??????????? ? ?????????????, ??? ??? ?????????? ?????????? ?????????? ? ??? ???????????? ????? ???????? ?? ???????? ????????? ?????????? ????? PCN ? SCN.

9. Связность и жизненный цикл SCN

? ???????????? ?????????? ????????? ???????? ?????????? ????? (???????? ????, ?????? ???????, ?????????? ????????) ? ?? ???????????: ??? ?????????? ? ???????????? ?????? ?? PCN, ????? ??????? ????????? ??????????? ? ?????????? ??????????, ? ??? ???????? ????????? ??????????????.

???????????? ??????: ??????? «???????? ????????????» (??? ???????? ????? ? ?????????? ??? ??????? ?????? ? ??? ?????? ?????) ? ???????? ?????? ?? ?????????? ?????????? (???? ??? ????).

Cheat Sheet по интеграциям KATA с KUMA

Введение

? KATA ?????? 7.0 ????????? ????? ??????????? ? ?????????? ? KUMA. ?????? ?????? ?????????? ?? ????????? ?????????? ?????? ??????????, ? ????? ????????? ?? ????? ???????? ???? ?????????? ?? ????????????????? ?????? ??????.

Схема взаимодействия

image.png

Подробнее

Что такое KATA Alerts?

??????? Alerts ? ???-?????????? KATA

image.png

Что такое User activity?

??????? Logs - User activity ? ?????????? KATA

image.png

??? ????????? ???????? ??????? ? ???????? ????????????? KATA ? KUMA - ??????

Что такое EDR telemetry?

??????? Threat hunting ? ???-?????????? KATA

image.png

??? ????????? ???????? ?????????? EDR ? KUMA - ??????

Что такое NDR events?

??????? Network traffic events ? ???-?????????? KATA

image.png

Что такое NDR Audit?

??????? Logs - Audit ? ???-?????????? KATA

image.png

Что такое NDR Application messages?

??????? Logs - Application messages ? ???-?????????? KATA

image.png

??? ????????? ???????? ???????, ?????? ? ????????? NDR ? KUMA - ??????

Что такое NDR Assets?

??????? Assets ? ???-?????????? KATA

image.png

??? ????????? ???????? ???????, ???????????? NDR ? KUMA - ??????