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

- Маркетинговые материалы
- KATA в распределённой инсталляции (PCN/SCN): принцип работы и эксплуатационные особенности
- Cheat Sheet по интеграциям KATA с KUMA

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

?????? ?????? ???????? ?????? ?? ????????????? ????????? ?? ???????? KATA&KEDR&NDR. ??? ????????? ???????????? ? ???? ?????? ??? ??????????.

Основные материалы:

- Страница сайта KATAP - ссылка
- Страница сайта KEDR - ссылка
- Datasheet KATA – ссылка
- Datasheet KEDR – ссылка
- Листовка Why KATA? – ссылка
- Ценность для бизнеса от внедрения KATA – ссылка
- Ценность для бизнеса от внедрения KATA/KEDR – ссылка
- Листовка How to sell – ссылка
- What’s new KATA&KEDR – ссылка

Видеоролики:

- Обучающие видео по Kaspersky Anti Targeted Attack Platform - ссылка

Истории успеха/Россия и СНГ:

- Кумтор – ссылка
- РН-БашНИПИнефть – ссылка
- Head Hunter – ссылка
- Фосагро – ссылка
- Магнит – ссылка
- МКБ – ссылка
- Правительство Ростовской области – ссылка
- Центральная пригородная пассажирская компания – ссылка
- Инфосистемы Джет – ссылка
- KICB – ссылка
- Новосталь-М – ссылка

- Компания нефтегазового сектора – ссылка
- Азиатский газопровод – ссылка
- РТИ Системы – ссылка
- Оптима Банк – ссылка

Материалы по запросу:
Дополнительные материалы вы можете запросить через почту у команды pre-sale инженеров AntiAPT.

KATA ? ??????????????? ??????????? (PCN/SCN): ??????? ?????? ? ???????????????? ???????????

> **Примечание.** Материал подготовлен для AntiAPT Community и предназначен для практического понимания принципов работы. Он не заменяет официальную документацию вендора.

Распределённая инсталляция Kaspersky Anti Targeted Attack Platform (KATA) применяется, когда требуется единый контур управления для нескольких площадок/подразделений и/или масштабирование по количеству активов и объёму анализируемых данных.

??????????

9. Связность и жизненный цикл SCN

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

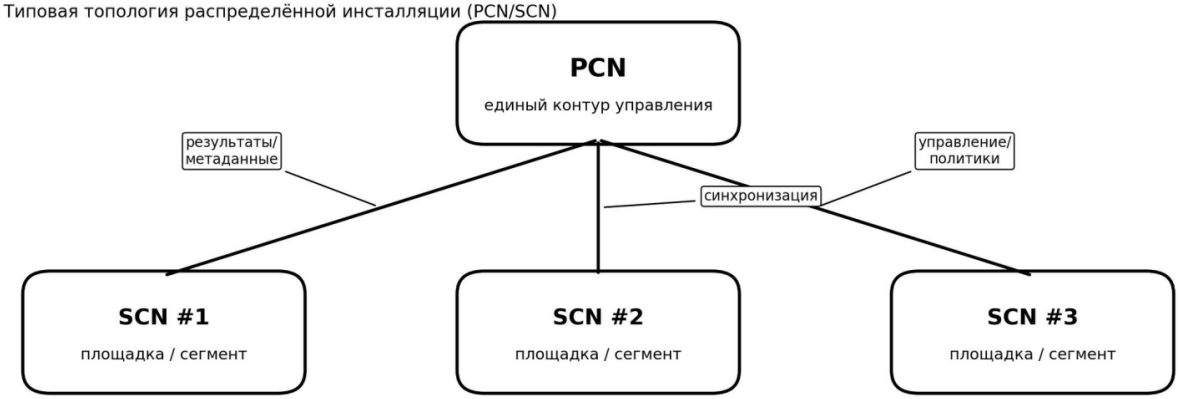
В распределённой инсталляции несколько серверов Central Node работают как единая система: управление централизуется, а обработка данных выполняется ближе к источникам событий (по площадкам/сегментам/тенантам).

Как правило, распределённый режим выбирают при масштабировании (по активам и трафику), а также при необходимости разграничить инфраструктуру по филиалам или по тенантам.

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

- **PCN (Primary Central Node)** — главный сервер управления. Обычно является «точкой обзора» по всем подключённым площадкам.
- **SCN (Secondary Central Node)** — подчинённый сервер. Как правило, обслуживает «локальную» площадку и синхронизирует результаты с PCN.
- **Тенант** — логическая единица (организация/филиал), для которой ведётся раздельный контур данных и управления (в режиме мультитенантности).

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



3. ??? ?????????????? ?????????? ? ??????

В распределённой инсталляции PCN выполняет роль центральной точки управления, а SCN — роль площадочных узлов. При этом часть объектов и настроек централизуется, но сохраняется принцип «объект редактируется там, где создан».

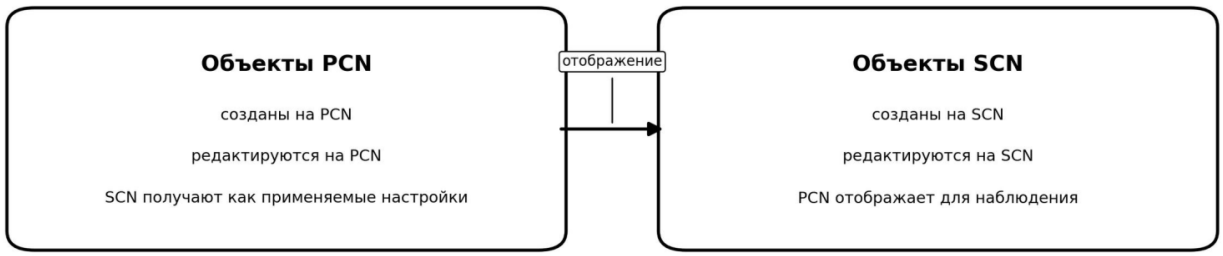
3.1. ??? ?????? ?????????????? ?? PCN

На практике на PCN удобнее вести единые политики, задачи и правила, а также контролировать алерты и результаты расследований по всей инсталляции. PCN выступает «витриной» по данным, которые поступают от SCN.

3.2. ??????? «??????? ????? — ????????????? ?????»

В эксплуатации важно заранее договориться о правилах администрирования: если объект создан на PCN, его жизненный цикл управляется на PCN; если объект создан на SCN — изменения выполняются на соответствующем SCN. Это снижает риск конфликтов и упрощает ответственность между командами/площадками.

Схема 2. Принцип «создано здесь — редактируется здесь»



4. ?????? ??????: ?????? ? Threat Hunting

SCN выполняют сбор и обработку данных в рамках своей площадки. Результаты (события/корреляции/детекты/метаданные) используются для формирования общей картины на PCN.

- **Алерты** агрегируются на уровне PCN для централизованного контроля и triage.
- **Threat Hunting** в распределённой инсталляции следует воспринимать как «единый поиск» по площадкам: запрос инициируется из центрального интерфейса, а результаты собираются из подключённых узлов.

5. ?????????, ????? ? ??????

Для эксплуатационной модели важно разделить роли: центральные администраторы (PCN) и площадочные операторы (SCN). В типовом сценарии учётные записи и роли администрируются централизованно, а доступ к конкретным площадкам ограничивается правами.

Отдельно имеет смысл учитывать ограничения по одновременным сессиям и правила доступа операторов к площадкам, чтобы избежать «технических конфликтов» при сменах и расследованиях.

6. ????????? ? ??????????????

В распределённой инсталляции необходимо заранее оценить влияние объёмов хранилища и лицензирования на площадочных узлах: даже при централизованном управлении объёмы данных и нагрузка зависят от того, какие источники подключены на конкретном SCN.

Практика: на этапе проектирования полезно фиксировать, какие типы данных хранятся и как долго (retention), отдельно для центрального уровня и площадок.

7. ???????????? SCN ? PCN: ??????? ? ???????????

Подключение SCN к PCN — это установление доверенного канала управления. В типовом процессе присутствует шаг верификации (например, сравнение отпечатка сертификата), который позволяет исключить подключение к «не тому» центральному узлу.

> **Важно.** Рекомендуется заранее определить регламент: кто создаёт учётную запись для подключения SCN, кто выполняет сверку отпечатка сертификата (вне канала), и кто уполномочен подтверждать подключения площадок.

8. ????????? ???????????: ?????? ???????????

Для распределённой инсталляции следует отдельно описать процедуру резервного копирования и восстановления, так как доступность резервного копирования и его корректность могут зависеть от текущего состояния подключений между PCN и SCN.

9. ????????? ? ????????? ???? SCN

В эксплуатации необходимо учитывать сценарии деградации связи (плановые окна, аварии каналов, разделение площадки) и их последствия: что происходит с отображением данных на PCN, какие статусы считаются нормальными в переходных состояниях, и как выглядит регламент восстановления.

Практический подход: описать «критерии нормальности» (что оператор видит в интерфейсе при штатной работе и при потере связи) и добавить ссылки на внутренние регламенты (если они есть).

Cheat Sheet ?? ??????????? KATA с KUMA

????????

В KATA версии 7.0 появились новые возможности и интеграции с KUMA. Данная статья направлена на упрощение восприятия данных интеграций, а также агрегации на одной странице всех инструкций по взаимодействию данных систем.

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

image.png

?????????

Что такое KATA Alerts?

Вкладка Alerts в веб-интерфейсе KATA

image.png

Что такое User activity?

Вкладка Logs - User activity в интерфейсе KATA

image.png

Как настроить отправку алертов и действий пользователей KATA в KUMA - ссылка

Что такое EDR telemetry?

Вкладка Threat hunting в веб-интерфейсе KATA

image.png

Как настроить отправку телеметрии EDR в KUMA - ссылка

Что такое NDR events?

Вкладка Network traffic events в веб-интерфейсе KATA

image.png

Что такое NDR Audit?

Вкладка Logs - Audit в веб-интерфейсе KATA

image.png

Что такое NDR Application messages?

Вкладка Logs - Application messages в веб-интерфейсе KATA

image.png

Как настроить отправку событий, аудита и сообщений NDR в KUMA - ссылка

Что такое NDR Assets?

Вкладка Assets в веб-интерфейсе KATA

image.png

Как настроить передачу активов, обнаруженных NDR в KUMA - ссылка