Вопросы и ответы с вебинара «КриптоПро Центр Мониторинга». Интеллектуальный мониторинг работоспособности компонентов PKI-инфраструктуры, средств электронной подписи и удаленного доступа» от 13.09.2019 г.

1. Прошу поподробнее рассказать про мониторинг VPN NGate?
В тестах для NGate есть проверка, связанная непосредственно с сервисом VPN.

2.Планируется ли использование слепой подписи для сохранения конфиденциальности документов, отправляемых на подпись HSM?
Не планируется.

3. Возможна ли интеграция с SIEM? Если да, то с какими?
На данный момент интеграция возможна путём выгрузки логов. Т.е. с любыми SIEM, которые это поддерживают.

4. Сервер мониторинга на какой OS функционирует?
Windows Server 2008 R2/2012/2012R2 (x64)/2016.

5. А планируется ли в будущем перевести на отечественную OS?
Да, в случае перевода других наших продуктов на отечественную ОС.

6. Возможно ли работать с CSP 5.0 на Windows Server 2008 R2?
Да.

7. Между компонентами трафик шифрованный? Взаимодействие по какому протоколу происходит между агентом и сервером?
На данный момент траффик незашифрованный. Реализация такой возможности в планах есть. На данный момент: HTTP REST.

8. Регуляторы не будут возражать против установки на серверы ПАК УЦ доп. ПО, не относящегося к функционалу ПАК УЦ? (агент ЦМ)
В будущих сертификациях УЦ планируем явно прописать в документации такую возможность.

9. Для NGate нужен один агент на кластер или на каждый узел Ngate отдельный агент ставить/покупать?
Агент на кластер.

10. Интересует интеграция Центра Мониторинга с корпоративной системой мониторинга Компании, т.к. именно на нее завязан процесс заведения инцидентов ITSM системы и их решение в рамках зоны ответственности разных подразделений (Сетевики, инфраструктурщики, интеграция, ...) - в зависимости от типа инцидента – процесс решения инцидента идет по разным сценариям.
Интеграция на данный момент возможна с помощью:

- Предоставления лога ПК Центра Мониторинга
- Через программный интерфейс с использованием REST
- Отправка уведомлений через SMS и Email

11. Реализован ли в текущей версии ЦМ функционал по мониторингу Гаммы на HSM, т.к. гамма может закончиться в самый неожиданный момент?
Да, такой тест есть с возможностью предупреждения об истечении гаммы за N ключей.

12. Не будет ли нарушение эксплуатационной документации на HSM при организации мониторинга параметров работы HSM?
Мониторинг работает через штатные механизмы HSM, нарушений нет.

13. Можно ли подключить ЦМ к Zabbix? Можно ли отправлять сообщения в Телеграм?
Zabbix - да. Телеграм - сейчас нет, но можно самостоятельно написать плагин для этих целей. API очень простое. В том числе и для Whatsapp.

14. Нет ли ограничений при организации интеграции ЦМ с корпоративной системой мониторинга, связанных с исходящими правилами на МЭ из выделенного сетевого сегмента УЦ и DSS?
Формальных строгих ограничений (по документации) нет. Тем не менее, правила на МЭ надо настраивать с учётом практических требований по безопасности.

15. Как обойти ограничение по проверке подписания документов из ЦМ тестового пользователя с типом подписи УКЭП (Усиленная Квалифицированная ЭП). В данном случае происходит не подтвержденное волеизъявлением пользователя использование ключа ЭП для УКЭП.
Для мониторинга выпускается тестовый неквалифицированный сертификат.

16. Мониторится ли служба хранения ключей центра сертификации и загружены ли ключи в нее?
Отдельной проверки нет, но данную информацию можно получить при выполнении теста доступности с ЦС на Агенте Сервера ЦР.

17. Передается ли между агентом и сервером ЦМ информация ограниченного доступа?
Нет, там передаются события мониторинга.

18. Коллеги, вы говорили, что проверки OCSP/TSP работают через ocsputil /tsputil, которые обычно требуют клиентских лицензий. Они входят в комплект Центра Мониторинга?
В комплект Центра Мониторинга не входят, но если агенты установлены непосредственно на сервера со Службами УЦ, то лицензии на клиенты ocsp, tsp уже есть.

19. Когда будет реализован ЦМ для УЦ СМЭВ? Приблизительные сроки уже есть?
Ориентировочный срок: 2-3 месяца.

20. Скажите пожалуйста, каким-то образом сохраняется конфиденциальность подписываемых документов, отправляемых на подпись HSM

Не до конца понятен вопрос, ели рассматривать систему как: клиент HSM, ПАКМ HSM, система, обрабатывающая информацию, которая подключена к HSM, где компоненты работают в одном сегменте сети (в одной контролируемой зоне) и выполняются все требования с соответствующим классом защиты.

21. Проводилось ли нагрузочное тестирование (влияет ли на производительность ПАК КриптоПро У)?

Специального нагрузочного тестирования не проводили, так как проверки, выполняемые раз в 5-15 минут, не оказывают влияния на производительность компонент УЦ.

22. Возможно ли устанавливать агенты на географически удаленные компоненты УЦ?

Возможно. Надо будет обеспечить связность агентов к серверу Центра Мониторинга. Либо развернуть агенты и сервер в каждом ЦОД.

23. Как смс информирование реализовано? Необходим ли сторонний сервис?

В составе ПК Центр Мониторинга реализованы плагины для отправки SMS с поддержкой протокола SMPP. Отдельно реализованы плагины для взаимодействия с МТС коммуникатором и MFM – шлюзом.

Да, сторонний сервис необходим. Если Ваш шлюз для отправки SMS предоставляет особый интерфейс, то реализовать плагин для взаимодействия с ним будет достаточно просто в виду простой реализации интеграции по API.

24. Реализованы ли проекты с интеграцией ЦМ с Microsoft System center operations manager?

Практической реализации не было, но не видим существенных различий и ограничений при интеграции по аналогии с другими корпоративными системами мониторинга.

25. Вопрос не по теме, в начале вебинара упомянули что лицензия от CSP4 подходит для CSP5. Где об этом можно прочитать на сайте. Спасибо

Для получения информации Вы можете отправить письмо по адресу info@cryptopro.ru.