ПРОТОКОЛ № 25565/2024

проведения совместных испытаний программного обеспечения "Security Capsule SIEM" версии 3.3 и программного изделия СУБД "Tantor SE" версии 16.2.1

г. Санкт-Петербург 22.10.2024

1 Предмет испытаний

1.1 В настоящем протоколе зафиксирован факт проведения в период с 21.10.2024 по 22.10.2024 совместных испытаний программного обеспечения "Security Capsule SIEM" версии 3.3, разработанного ООО «ИТБ», и программного изделия СУБД "Tantor SE" версии 16.2.1, разработанного ООО "ТАНТОР ЛАБС".

2 Объект испытаний

2.1 Перечень компонентов, эксплуатировавшихся в ходе проведения данных испытаний представлен в Таблице 1.

Таблица 1 – Перечень пакетов дистрибутива

Описание	**Наименование дистрибутива**	**MD5**	**Источник**
Файл программного пакета дистрибутива "Security Capsule SIEM" версии 3.3	siemwebapplicationcert.tar.gz	bf28f6732a8232f65ecbd2a1be7160d8	Сторона разработчика ПО
Файл программного пакета дистрибутива СУБД "Tantor SE" версии 16.2.1	tantor-se-server-16_16.2.1_amd64.deb	b89ef4af9b6364ad54faf129b2cebaac	Сторона разработчика ПО

3 Ход испытаний

3.1 В ходе проведения настоящих испытаний были выполнены проверки корректности совместного функционирования СУБД "Tantor SE" и "Security Capsule SIEM" версии 3.3 в объеме, указанном в Приложении 1.

3.2 В ходе испытаний использовался тестовый стенд, описанный в Приложении 3.

4 Результаты испытаний

4.1 "Security Capsule SIEM" версии 3.3 корректно функционирует совместно с СУБД "Tantor SE".

5 Вывод

5.1 "Security Capsule SIEM" версии 3.3 и СУБД "Tantor SE" версии 16.2.1 совместимы, принимая во внимание информацию, содержащуюся в разделах 3, 4.

6 Состав рабочей группы и подписи сторон

6.1 Данный протокол составлен участниками рабочей группы:

Графов Сергей Александрович – Руководитель проекта ООО «ИТБ»;

Жорин Андрей Александрович – Главный специалист отдела внедрения ООО «ИТБ».

ООО «ИТБ»

Руководитель проекта

(должность)

(подпись)

Графов С.А.

(фамилия, инициалы)

Приложение 1 к Протоколу № 25565/2024

Перечень проверок совместимости "Security Capsule SIEM" версии 3.3 и СУБД "Tantor SE"

№ п/п	Наименование проверки	Результат проверки
1.	Инициализация соединения с СУБД "Tantor SE"	Успешно
2.	Функциональное тестирование	Успешно

Приложение 2 к Протоколу № 25565/2024

Инструкция по интеграции "Security Capsule SIEM" версии 3.3
с СУБД "Tantor SE"

1 Настройка "Security Capsule SIEM" версии 3.3:

1.1 Создать новую подсеть для контейнеров:

docker network create --opt com.docker.network.bridge.name=br000 --driver bridge --subnet 172.16.211.0/26 siem_net

1.2 Изменить настройки файла "sim/appsettings.json", указав ip адрес подключения к СУБД "Tantor SE", логин и пароль пользователя с правами на создание, запись и чтение.

1.3 Создать и запустить контейнер (после выполнения настройки СУБД):

docker run -itd --name siemwebappcert-srv -e .env --network siem_net --device=/dev/bus/usb/001/003 -p 0.0.0.0:8000:80 -v /home/u/siem/siemwebapplication/siem/appsettings.json:/app/appsettings.json -v /home/u/siem/siemwebapplication/siem/appsettings.enc:/app/appsettings.enc -v /home/u/siem/siemwebapplication/siem/logs:/app/logs siemwebapplication:latest

2 Настройка СУБД "Tantor SE":

2.1 Создать пользователя с правами на создание, запись и чтение, либо использовать существующего пользователя "postgres".

2.2 В файле "postgresql.conf" вместо "localhost" указать "*"

2.3 В файле "pg_hba.conf" "0.0.0.0" заменить на "172.16.211.0/26"

2.4 Перезапустить службу.

Приложение 3 к Протоколу № 25565/2024

Описание стенда

1. СУБД "Tantor SE" версии 16.2.1 запущенная в среде операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.7) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2023-1023SE17 (оперативное обновление 1.7.5) на ядре 6.1.50-1 generic.

2. "Security Capsule SIEM" версии 3.3 запущенная в среде операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.7) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2023-1023SE17 (оперативное обновление 1.7.5) на ядре 6.1.50-1 generic..

Приложение 4 к Протоколу № 25565/2024

Перечень используемых сокращений

СУБД – система управления базами данных;

ПО – программное обеспечение.