



VB-Trend 2025

АНТИХРУПКОСТЬ

БИЗНЕСА



Мельников Тимофей
ВолгаБлоб



Smart Code

альянс с Код Безопасности



Коростылев Павел
Код Безопасности

Код Безопасности в цифрах

30 лет

Защищаем крупнейшие
ИТ-инфраструктуры

1200+

Официальных партнеров

50000+

Организаций защищены нашими
продуктами

50+

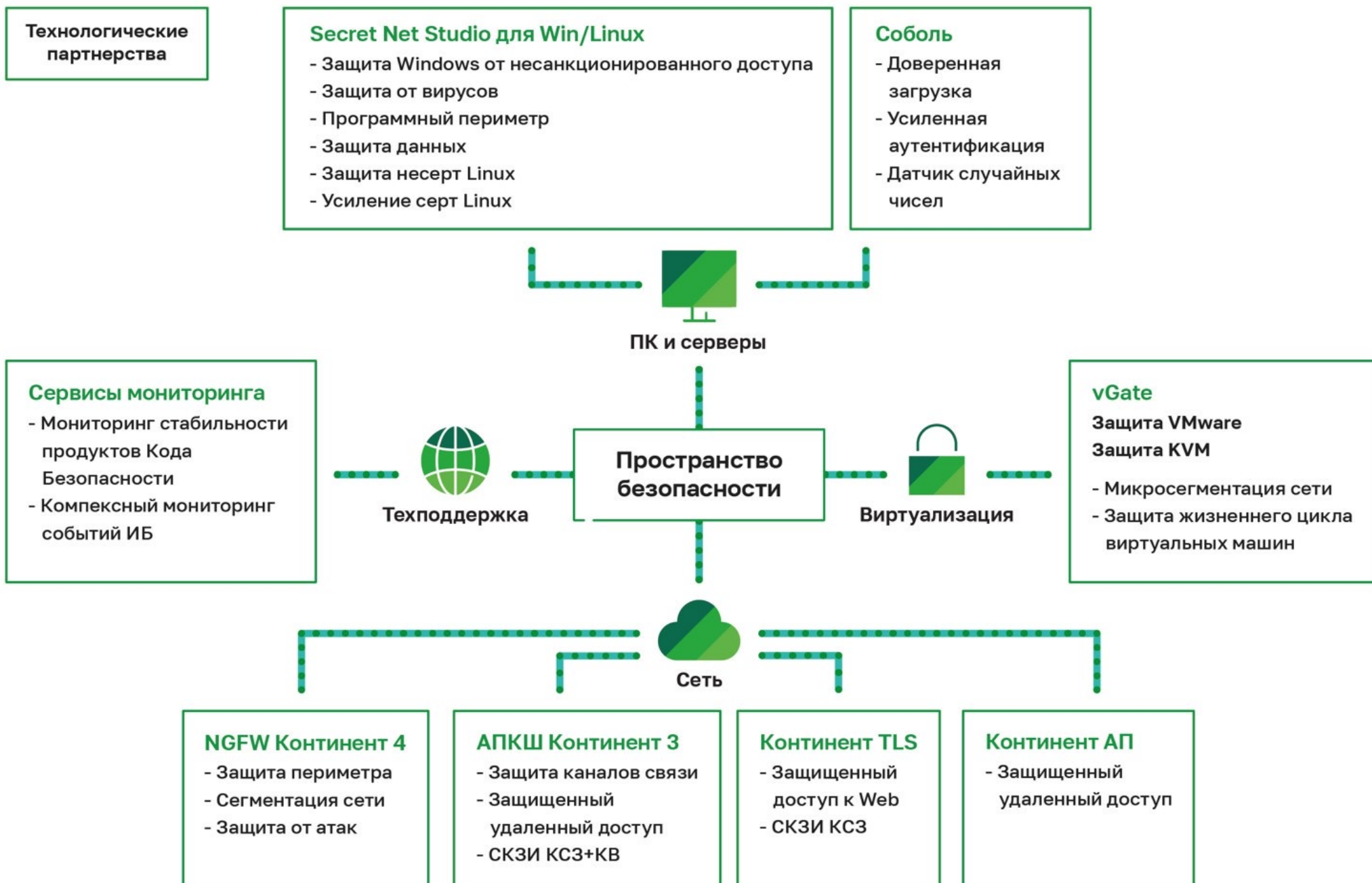
Разработанных средств защиты

60+

Лицензии и сертификаты ФСТЭК, ФСБ,
Минобороны России

1000+

Квалифицированных
специалистов



Что такое контентный модуль



Данные

компонентов
и информационных
систем



Системные логи



Событийный стриминг
функциональных компонентов



Метрики

Инфраструктурные
Функциональные



Справочники



Отчеты



Контент

набор готовых
инструментов



Здоровье



Функциональный
мониторинг



Интеграция с SM

Специализация продукта + SM
Обратная интеграция



Инвентаризация

Обогащения данных пользователями,
устройствами, компонентами



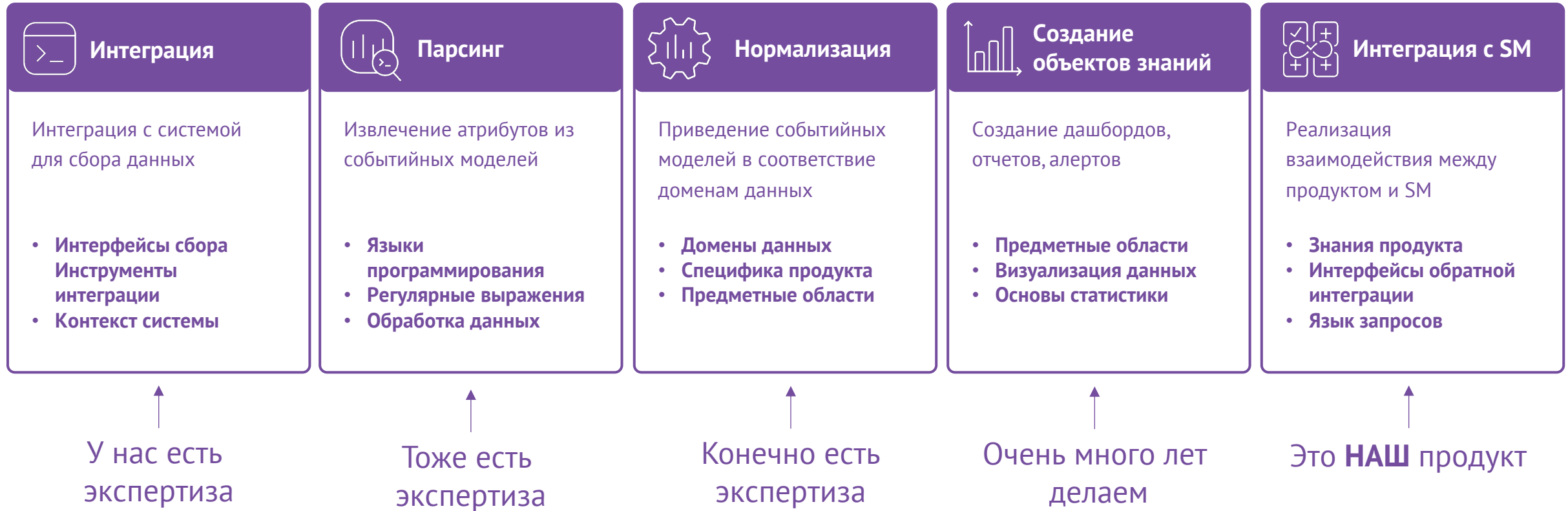
Информационная
безопасность

Профилирование, корреляционные
правила, TI

Это - контентный модуль

На каких этапах требуется наша экспертиза

Все же просто, зачем вы?

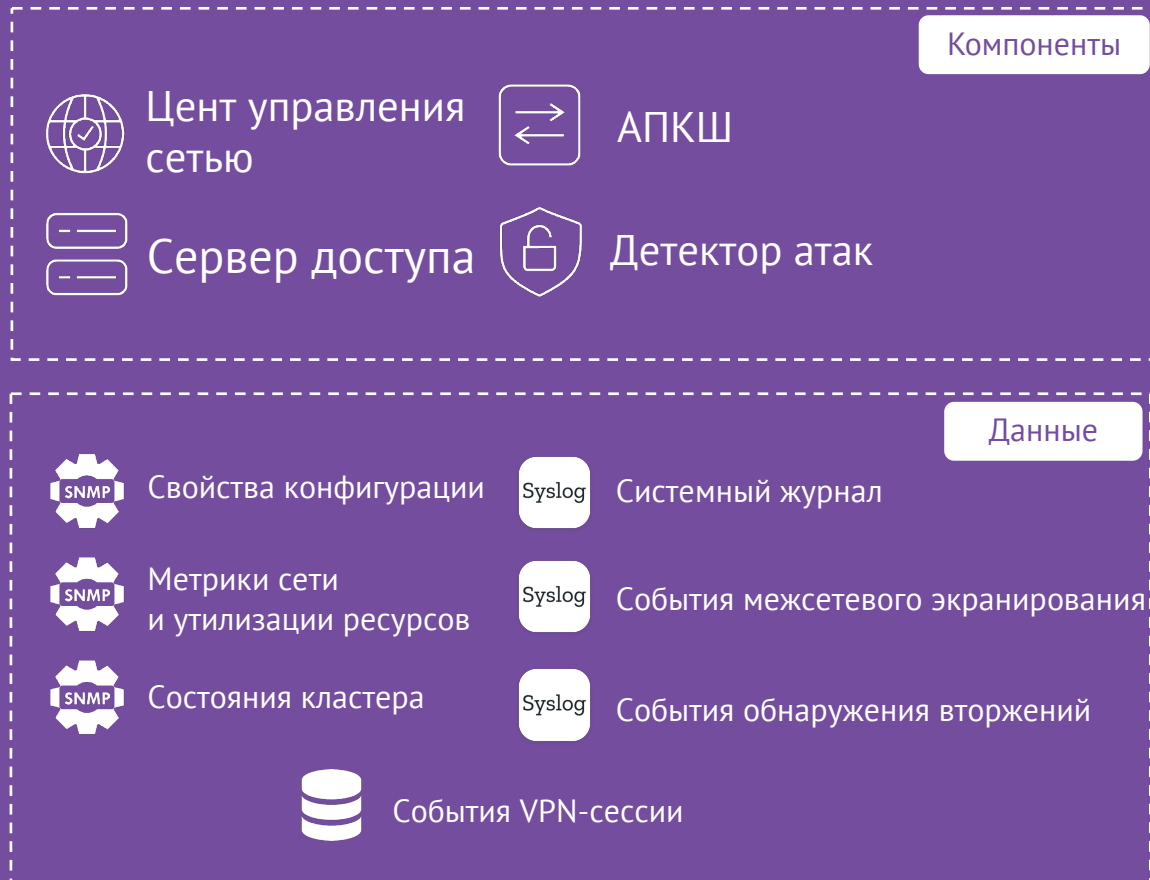


Вопрос: Можно сделать самому?

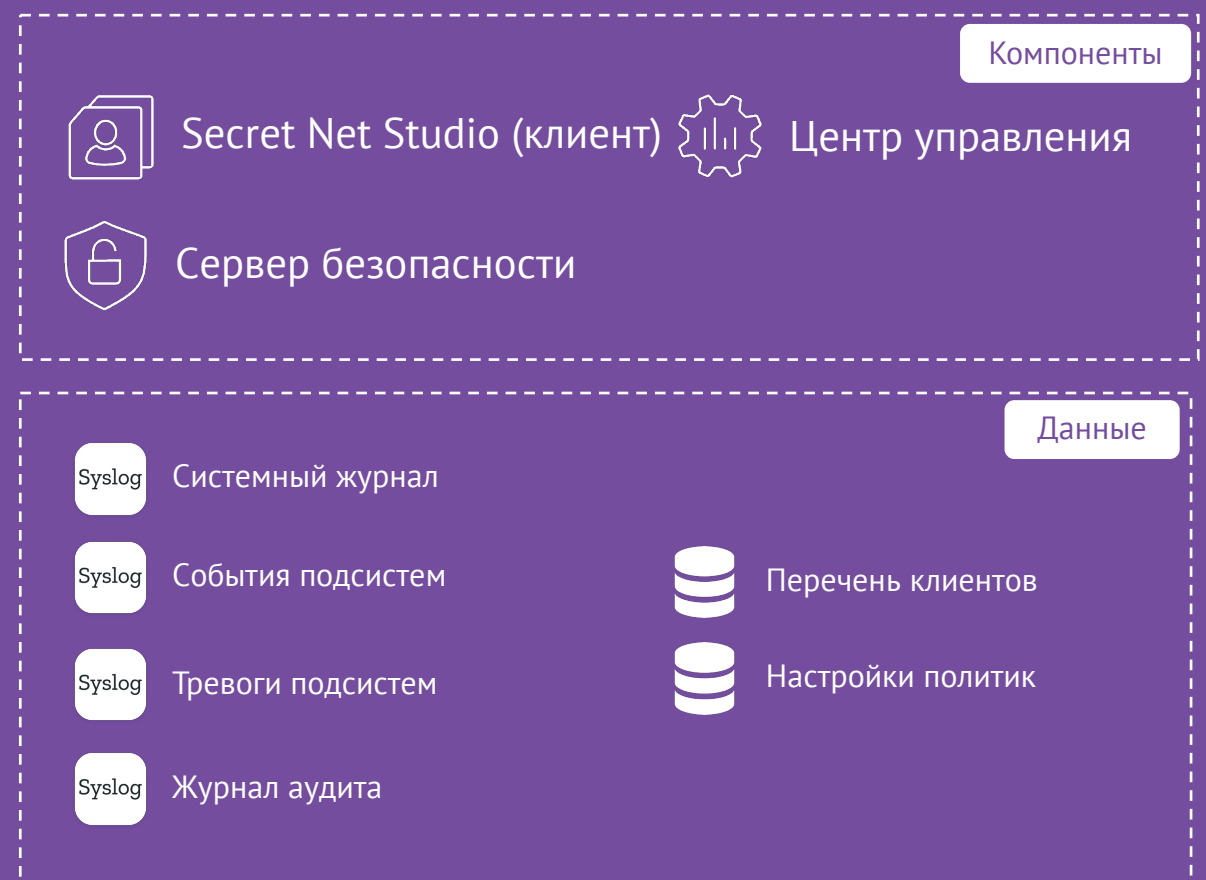
Ответ: Да, но зачем?

Smart Code: данные

Континент



Secret Net Studio

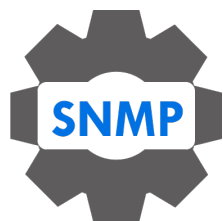


Smart Code: нормализация



Континент
Secret Net Studio

Syslog



Поставляют



Smart Monitor



Аутентификация



Обнаружение вторжений



Вредоносное ПО



Сеть



Управление учётными записями



Обработывает

Используют

Код безопасности

Континент

Secret Net Studio

Архитектура

Состояние
кластера

Режим работы

Статус узлов

Актуальность
ключей

Синхронизация

Статус
эксплуатации

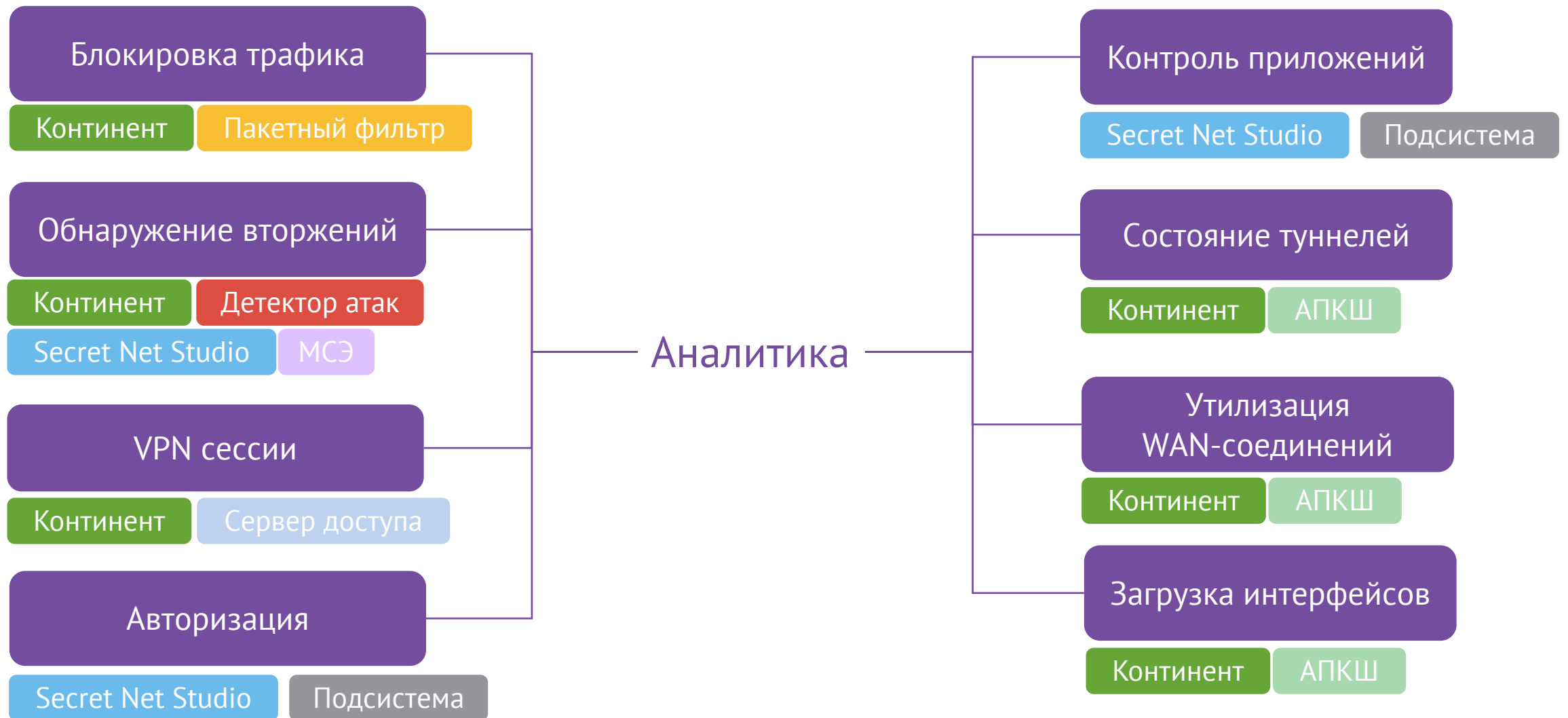
Состояние
подсистем

Состояние
сервера
безопасности

Лицензии

Статус
клиентов

Smart Code: аналитика функциональных возможностей



Smart Code: интеграция с модулями SM



Результаты

Smart Code

Архитектура и здоровье

Континент: Архитектура и конфигурация

Экспорт

Редактировать

Time

7 дней назад

Даты

Конфигурация кластера														
Столбцы Размер ячеек Сортировка На весь экран														
КШ	Тип	Кластериз...	Роль	Статус кла...	Местополо...	Шасси	Версия ко...	Владелец	Время раб...	Синхрониз...	Ключ узла	Статус эксп...	Мягкий ре...	
ЦУС: 67037 (172.16.0.121)	ЦУС	одиночный	-	-	StandCUS	IPC-25 (92D9)	142	TestAdminCUS	1 year	10 seconds	истек	введен в эксплуатацию	включен	
КШ: 66175 (172.16.0.122)	КШ	кластер	основной	активен	StandCluster	IPC-25 (92D9)	244	TestAdmin	4 days	5 seconds	активный (истечет через:	введен в эксплуатацию	выключен	
Детектор атак: 66176	Детектор атак	одиночный	-	-	IPS	IPC-25 (92D9)	121		3 days	16 seconds	активный (истечет через:	введен в эксплуатацию	выключен	
Сервер доступа: 67036	Сервер доступа	одиночный	-	-	SD	IPC-25 (92D9)	143		9 hours	13 seconds	активный (истечет через:	введен в эксплуатацию	выключен	

Multi-WAN						
Столбцы Размер ячеек Сортировка На весь экран						
КШ	ID WAN-канала	gateway	Время отклю...	Время недост...	Статус	
КШ: 66175 (172.16.0.122)	0	172.16.0.1	0 seconds	0 seconds	success	
КШ: 66175 (172.16.0.122)	2	192.192.192.1	4 days	4 days	failed	

Парные связи						
Столбцы Размер ячеек Сортировка На весь экран						
КШ	Парный КШ	Активные кан...	Каналы с оши...	Время отказа	Статус	
ЦУС: 67037	Сервер доступа:	5	0		success	
КШ: 66175	Сервер доступа:	5	0		success	
КШ: 66175	ЦУС: 67037	5	0		success	

Архитектура и здоровье

Континент: Состояние узла

Экспорт

✎ Редактировать

Time

АПКШ

📅

2025-04 → 2025-04

КШ: 66175 (172.1...

✕

▼

КШ

Тип конфигурации

кластер

Кластеризация

основной

Узел кластера

активен

Состояние основного узла

5 seconds

Синхронизация с ЦУС

актуален

Ключ узла

выключен

Мягкий режим

Конфигурация

🔧 Столбцы

📏 Размер ячеек

⬆ Сортировка

🖼 На весь экран

Параметр	Значение
IP адрес	172.16.0.122
Статус эксплуатации	введен в эксплуатацию
Владелец	TestAdmin
Версия сборки	3.9.3.3887
ОС	FreeBSD 11.3-STABLE
Ключ узла	активный (истечет через: 11 months)
Время работы	4 days
Шасси	IPC-25 (92D9)



Аналитика функциональных возможностей

Детектор атак: Обнаруженные вторжения

Экспорт

✎ Редактировать

Time

📅

2025-04 → 2025-04

108125

ВСЕГО

20

УСТРОЙСТВА

51

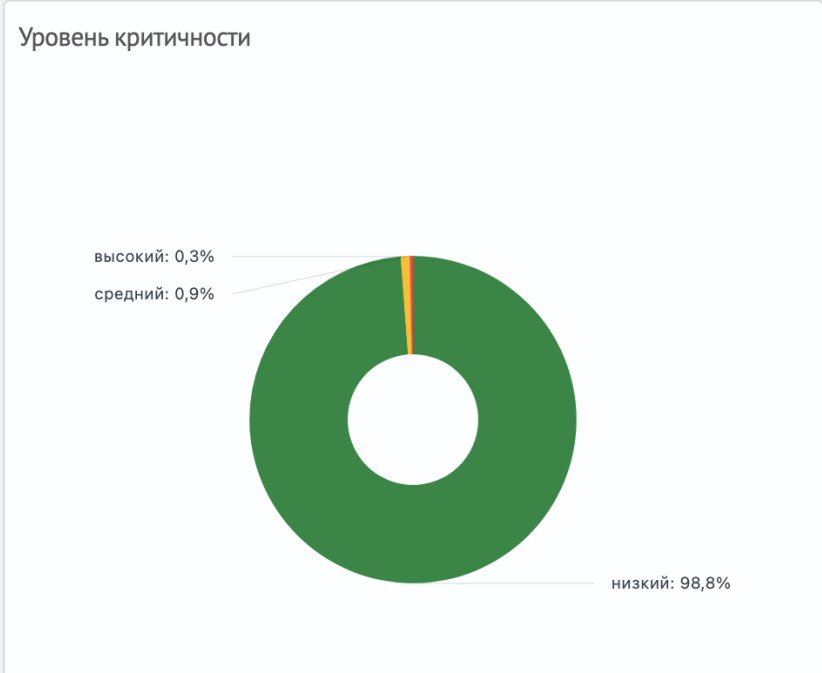
ВЫСОКИЙ

149

СРЕДНИЙ

16601

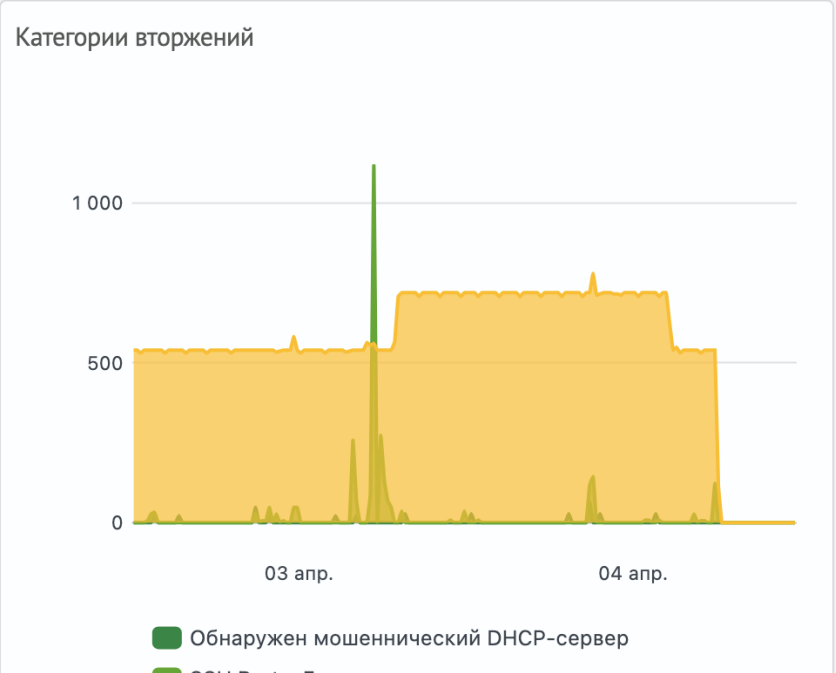
НИЗКИЙ



Вторжения в разрезе устройств

🖥 На весь экран

IP адрес	Высокий	Средний	Низкий	Вторжения
255.255.255.25	16	0	0	112
172.16.0.101	14	0	0	98
172.16.0.152	14	0	0	98
172.16.0.2	7	0	0	49
172.16.0.1	0	0	16586	104708
172.16.0.151	0	50	0	690
172.16.0.32	0	15	0	621
172.16.0.9	0	9	7	445



Аналитика функциональных возможностей

Secret Net Studio: Аудит и тревоги подсистем

Экспорт

Редактировать

Time

7 дней назад

Даты

APM

Все

Контроль приложений: статистика по APM

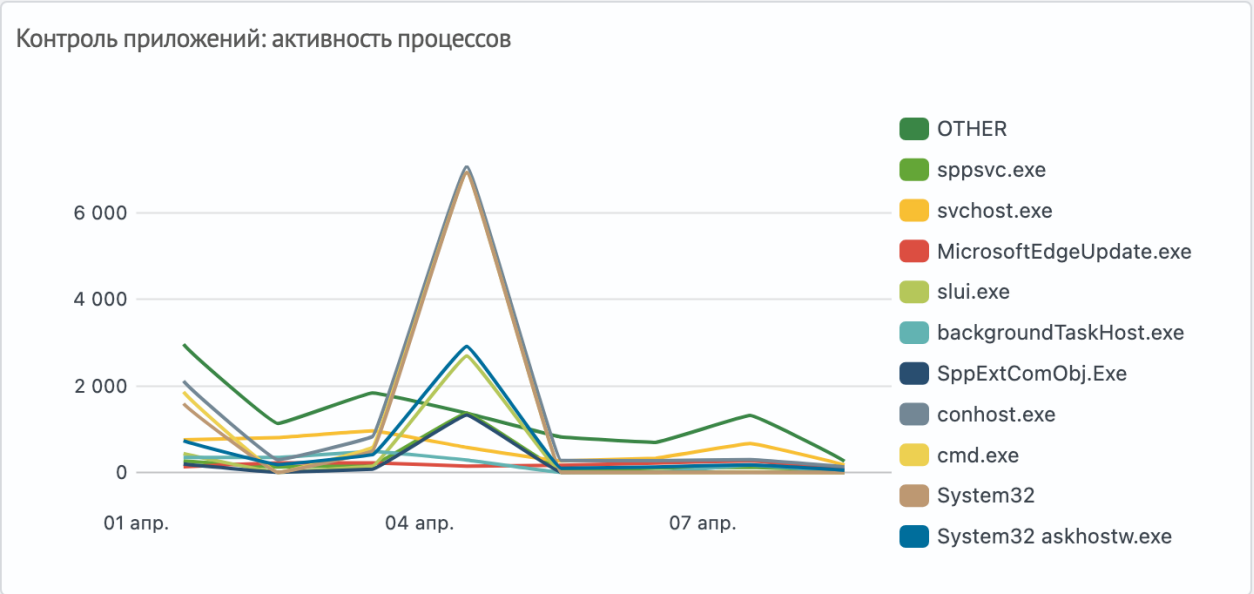
Столбцы

Размер ячеек

Сортировка

На весь экран

APM	Процессы	Пользователи	Запуски	Остановки
smartcode-2.test.local	161	16	20445	20442
smartcode-1.test.local	182	16	9288	9306



Контроль приложений: аудит процессов

Столбцы

Размер ячеек

Сортировка

На весь экран

@timestamp	Событие	APM	Пользователь	Домен	Процесс	ID Процессы	Директория	Родительский процесс
2025-04-	Завершение процесса	smartcode-1.test.local	СИСТЕМА	NT AUTHORITY	svchost.exe	7152	\Device\HarddiskVolume4\	
2025-04-	Завершение процесса	smartcode-1.test.local	СИСТЕМА	NT AUTHORITY	System32 askhostw.exe	6608	\Device\HarddiskVolume4\	
2025-04-	Запуск процесса	smartcode-1.test.local	NETWORK SERVICE	NT AUTHORITY	sppsvc.exe	8028	\Device\HarddiskVolume4\	services.exe

Код безопасности + инвентаризация

АПКШ Континент

Создать объект вручную

Базовые поля

Показать фильтры

Дополнительные поля

Показать фильтры

🔍 Поиск...

Выбранные поля

8

▼

host_geo_name	host_ip	soft_mode	reserve_state	host_id	cus_sync_dur	conf_type
StandCUS	172.16.0.121	включен	-	67037	10 seconds	ЦУС
StandCluster	172.16.0.122	выключен	активен	66175	5 seconds	КШ
IPS	172.16.0.117	выключен	-	66176	16 seconds	Детектор атак
SD	172.16.0.126	выключен	-	67036	13 seconds	Сервер доступа

Строк на странице: 10 ▼

Код безопасности + инвентаризация



Smart Monitor

Инвентаризация

АПКШ Континент

ЦУС: 67037 (172.16.0.121)



admin

ЦУС: 67037 (172.16.0.121)

Поля

Базовые

Поле	Значение
host_ip	172.16.0.121
host_id	67037

Дополнительные

Изменить дополнительные поля

Поле	Значение
host_geo_name	StandCUS
soft_mode	включен
build_version	3.9.3.3887
conf_version	-
reserve_state	-
expiry_key	0
cus_sync_dur	10 seconds

Связи



Показать карту связей

Код безопасности + инвентаризация

Связи



Показать карту связей

ЦУС: 67037 (172....) КШ: 66175 (172.16.0.122) -> ЦУС: 67037 (172.16.0.121)

Связанные активы Общая информация

Поиск

Исходящие

Входящие

Тип актива не выбран

Актив

Тип связи

Тип актива

▼

ЦУС: 67037 (172.16.0.121)

Родительский актив

Входящая

IP

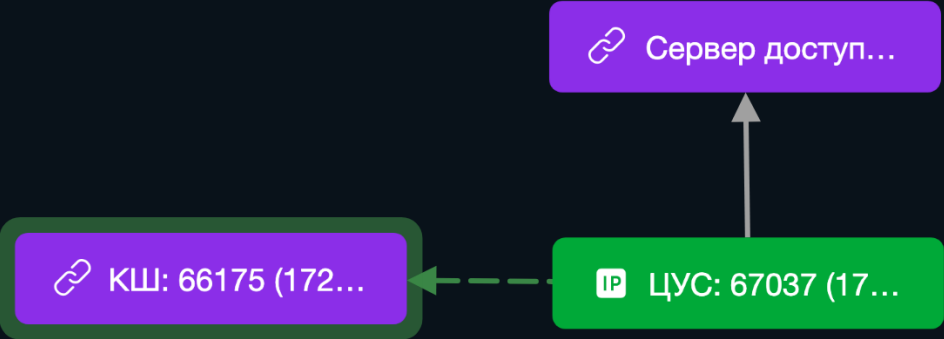
АПКШ Континент

Строк на странице: 25

<

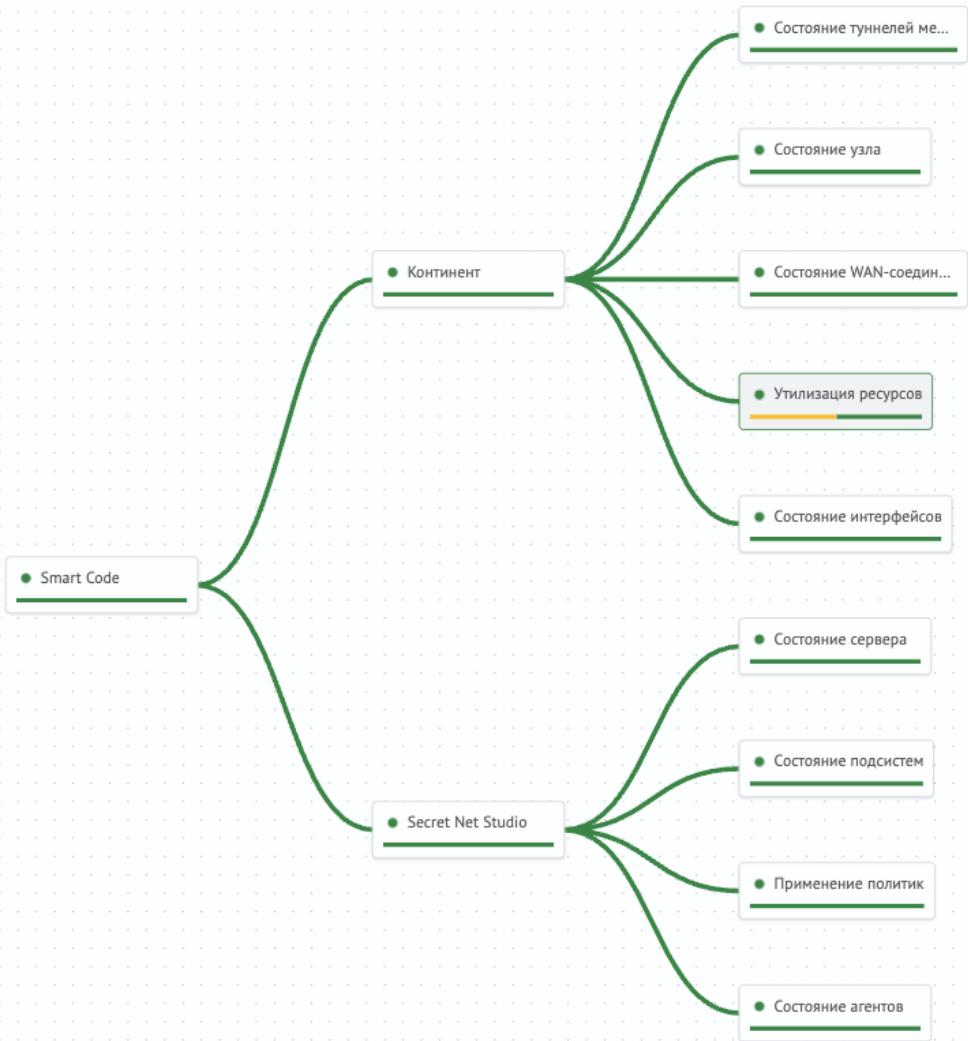
1

>



Код безопасности + РСМ

PCM



Утилизация ресурсов

95.83

Подробнее

Поиск

Критичность 7

Название	Значение
Утилизация CPU	0.39
Утилизация RAM	0.79

Спасибо
за внимание!

Приходите в демо-зону

