

РАССУЖДЕНИЕ О ДВУХ БРАТЬЯХ PSIM и SIEM



Назаров Фёдор

ПАО «ГМК «Норильский никель»

Кто они по документам?

PSIM – (от англ. Physical security information management — «управление информацией о физической безопасности») — категория программного обеспечения, предоставляющая аппаратно-программный комплекс для интеграции нескольких несвязанных между собой приложений и устройств безопасности и управления ими через единый пользовательский интерфейс.

SIEM – (Security information and event management) — объединение двух терминов, обозначающих область применения ПО: SIM (Security information management) — управление информацией о безопасности, и SEM (Security event management) — управление событиями безопасности.



Когда они родились?

Доподлинно не известно, но:



13-й век до н.э.

Рамсес I. Он реорганизовал армию. Была также создана специальная гвардия для охраны особы фараона.



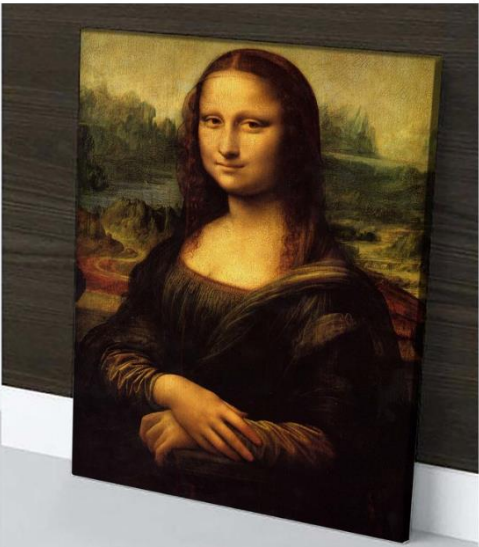
1-й век до н.э.

Шифр Цезаря. Юлий Цезарь использовал его, чтобы защищать информацию в военных сообщениях.

Они не близнецы. В чем они отличаются ?

КАЖДАЯ СЛЕДУЮЩАЯ КОПИЯ

—
Ценность все ниже и ниже



☆☆☆☆☆ 0 отзывов / Написать отзыв

Производители Red Panda
Доступность: На складе
Код товара: p51741
Ширина: 40 см x Высота: 60 см

2 490.00 р.

ДОСТУПНЫЕ ОПЦИИ

* Размер

30 40 ☐	60 40 ☐	70 50 ☐
80 ☐		



OC Linux & Unix
Astra Linux Special Edition

Доставка от 1 дня 2 ★★★★★

20 400 ₽

Выбрать лицензию

ХОТЬ 1000 КОПИЙ

—
Ценность не меняется

Они не близнецы. Давайте делиться!

Реализовано много
интересных концепций



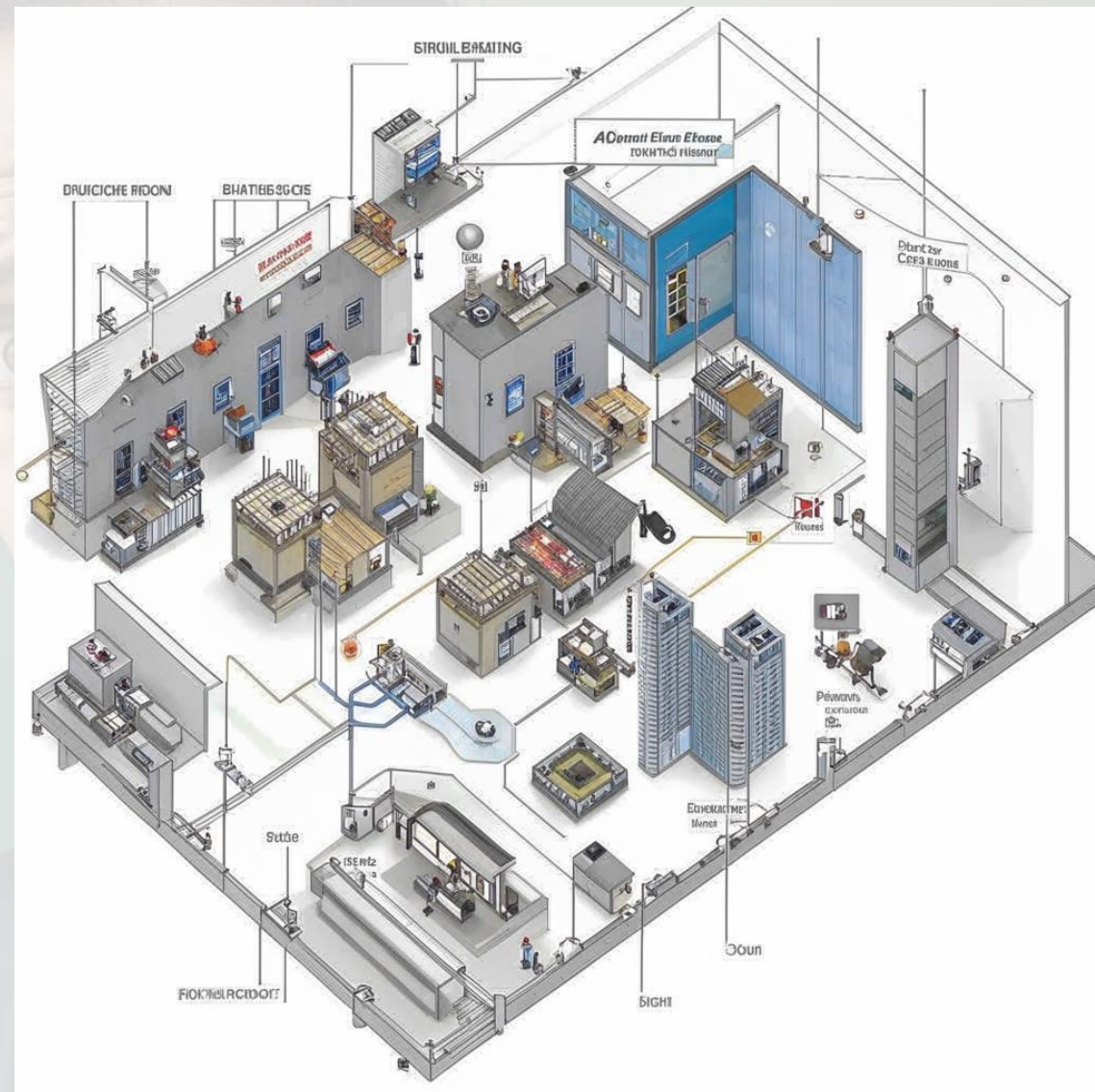
Стремление развиваться

Классная функция для PSIM (№1)

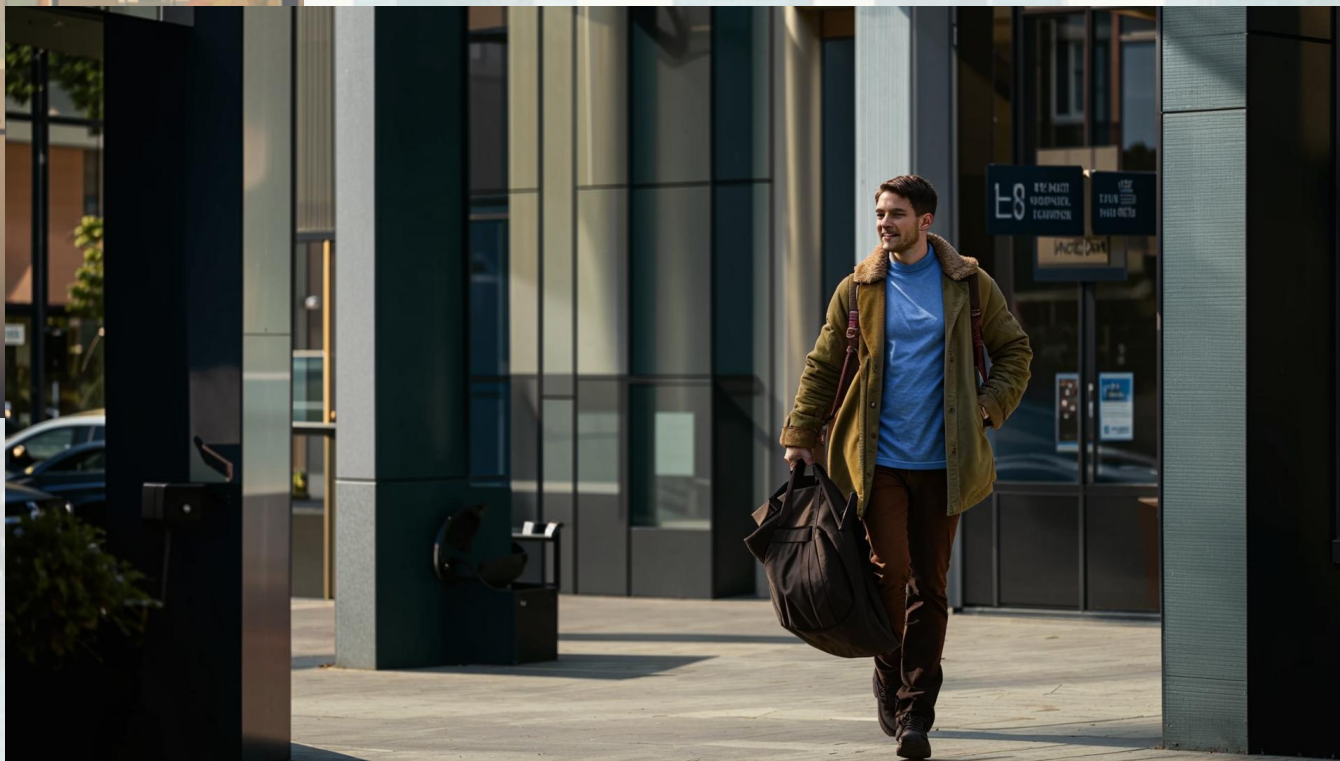
Я НЕ ХОЧУ БЕГАТЬ И ИСКАТЬ ЭКСПЛУАТАЦИОННУЮ ДОКУМЕНТАЦИЮ

А давайте PSIM сможет производить обследования сети КСБ на предмет устройств с открытым 554 портом (RTSP) и иных портов присущим системам безопасности.

А если у PSIM есть учетные данные к интерфейсам систем, то пусть она еще и производителя и специфику систем предоставляет пользователю.



Только этого мало. Как найти еще?



Классная функция для PSIM (№2)

**ЕСТЬ ШИКАРНАЯ КОНЦЕПЦИЯ!
ДАВАЙТЕ ПЕРЕИСПОЛЬЗУЕМ ЕЕ!**

В PSIM системах хранится ретроспективная информация от различных источников. Давайте запомним типичное поведение на участке/в сегменте и будет выявлять **Аномальное поведение**.

Пусть **Аномальное поведение** станет новым событием PSIM.



А кто из них преступник?



Сергей Пантелеевич Мавроди
«ПираМММида»

Фрэнк Уильям Абигнейл-младший
«Поймай меня, если сможешь»

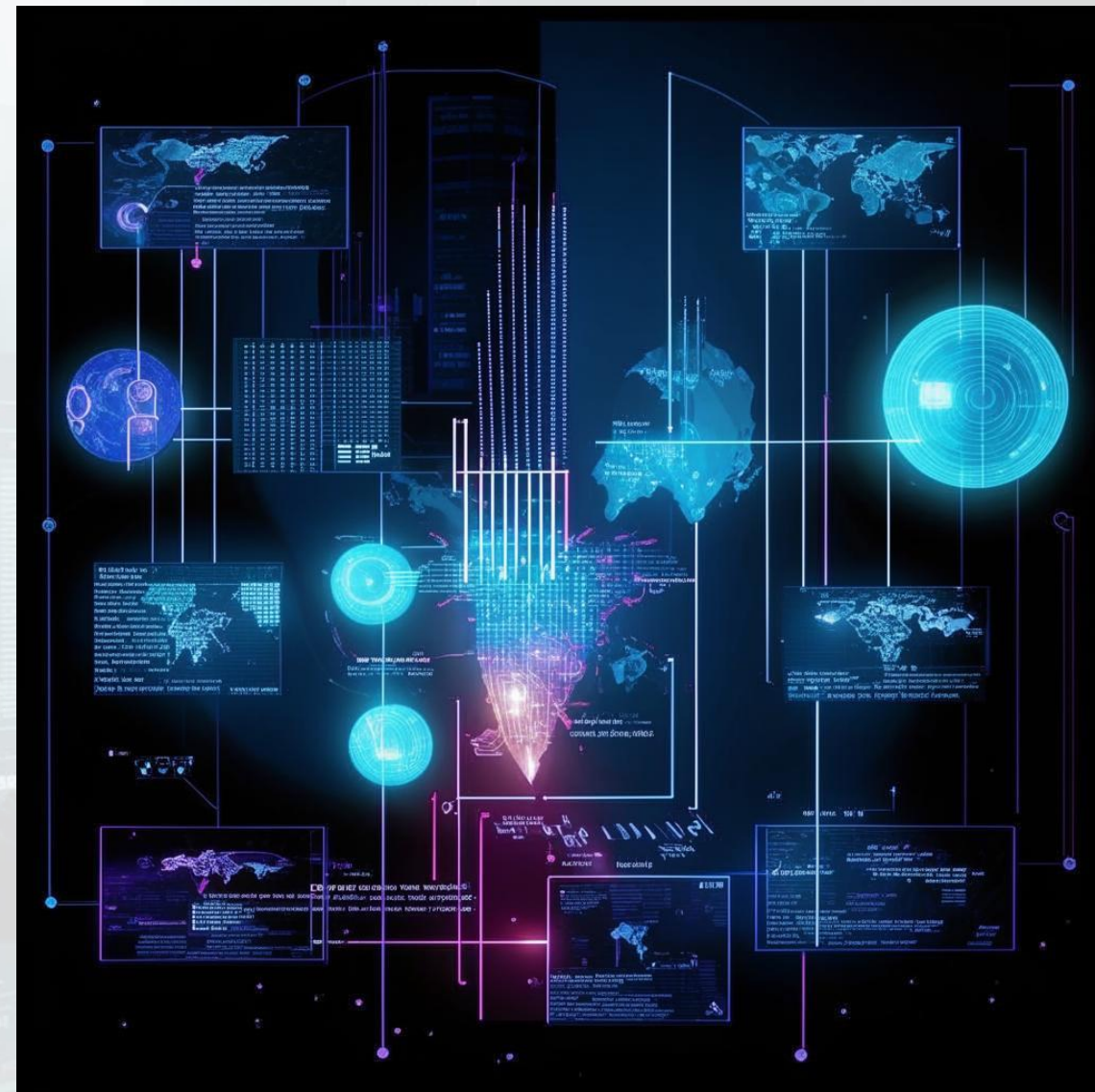


Классная функция для PSIM (№3)

ЗАЧЕМ ВЫ НА МЕНЯ ВОЗЛОЖИЛИ ЭТУ РУТИНУ

Коль в PSIM системах хранится ретроспективная информацию давайте применять **машинное обучение**.

А что если пометать сообщения многократно воспринятые как неважные **пониженным приоритетом**, а потом, если захочет пользователь, и вообще не показывать?

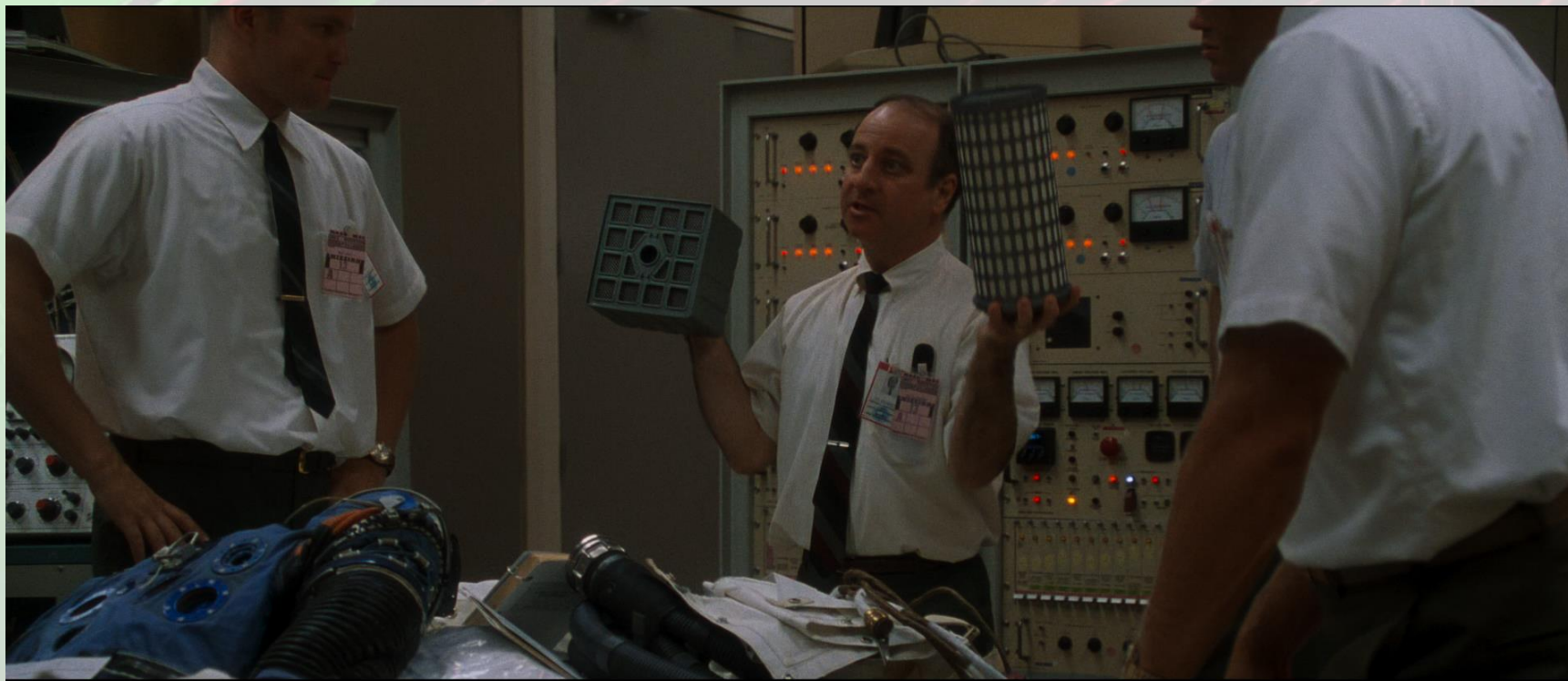


Крик души



**СОБИРАЙТЕ ДАННЫЕ!
ОНИ ВАМ ПОНАДОБЯТСЯ!**

Боль интеграции



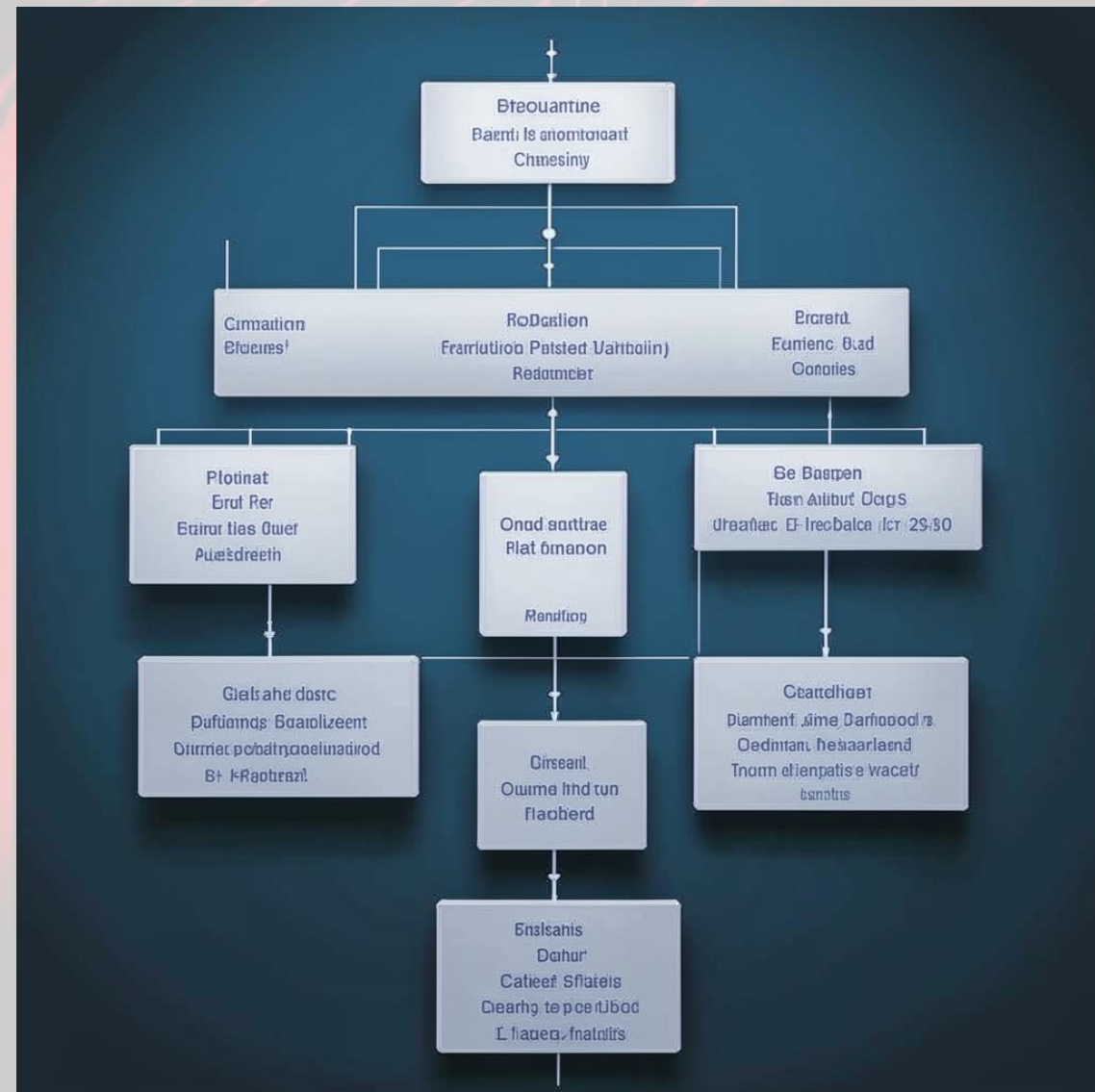
**ХОТИТЕ ВЗЯТЬ ДАННЫЕ ИЗ НЕСКОЛЬКИХ СИСТЕМ?
БУДЬТЕ ГОТОВЫ К СЮРПРИЗАМ!**

Классная функция для PSIM (№4)

**Люди любят стандарты.
Давайте их создавать вместе!**

Будет шикарно, если базовое описание событий в PSIM будет у всех производителей одинаковое.

Производители PSIM! Давайте обмениваться и публиковать таксономию описания событий объектовой безопасности.



Итог. Что будет полезно обоим?

- Знать, что вокруг не от человека, а определять самому.
- Знать, что нормально, а что аномально.
- Не бояться передать рутину компьютеру.
- Помнить, что большой объем данных компьютер обработает лучше человека.
- Говорить в одних терминах.

БЛАГОДАРИМ ЗА ВНИМАНИЕ

