SOC
FORUM
2023

Назад в будущее

КЛИЕНТСКИЙ ОПЫТ ВЫБОРА SIEM

Денис Андреевский
ООО ГЕФЕСТ ТЕХНОЛОДЖИЗ

Надоедливый клиент

SOC FORUM 2023

6 лет - 3 раза CISO

Выбор SIEM для: Банкинг, ИТ, Металлургия, Телеком

Когда деревья были большими

SOC FORUM 2023

- Штудирование документации вендоров
- Сведение параметров решений
- Интерпретации
- Значимые показатели / блок-факторы
- Закупки

Еще нет никаких операционных процессов ИБ, SLA, постанализ, риски – все настолько далеко!

Критическая информационная инфраструктура

SOC FORUM 2023

- Бизнес сегмент, АСУТП
- Координация с ИТ – стратегией
- Актуализированная модель угроз
- 60/40
- Функциональные требования
- Нюансы реализации

На пути к истине

SOC
FORUM
2023

SIEM в поле не воин

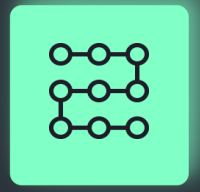
SOC FORUM 2023

Процессы

Use Cases

Ролевая модель

Отчетность
& Дашборды



Red Team
& Kill chain

SOC
FORUM
2023

В 5-ый раз в ту же воду?

Добродетели

SOC FORUM 2023

- Производительность
- Низкая стоимость владения
- Соответствие операционной модели ИБ
- Легкость обучения персонала
- Автоматизация
- Проактивность (TI)
- Обогащение

Драйверы изменились

SOC FORUM 2023

- Что такое Gartner, Forrester?))
- Доминирование государства (196)
- Геополитический фактор
- Смена источников (СЗИ и инфраструктура)
- Поиск ценового баланса
- Игра только в своей лиге

Chat GPT

SOC FORUM 2023

- Рисуем картины
- Пишем код на Python
- ...
- Фреймворк атак на инфраструктуру?

SOC
FORUM
2023

Спасибо