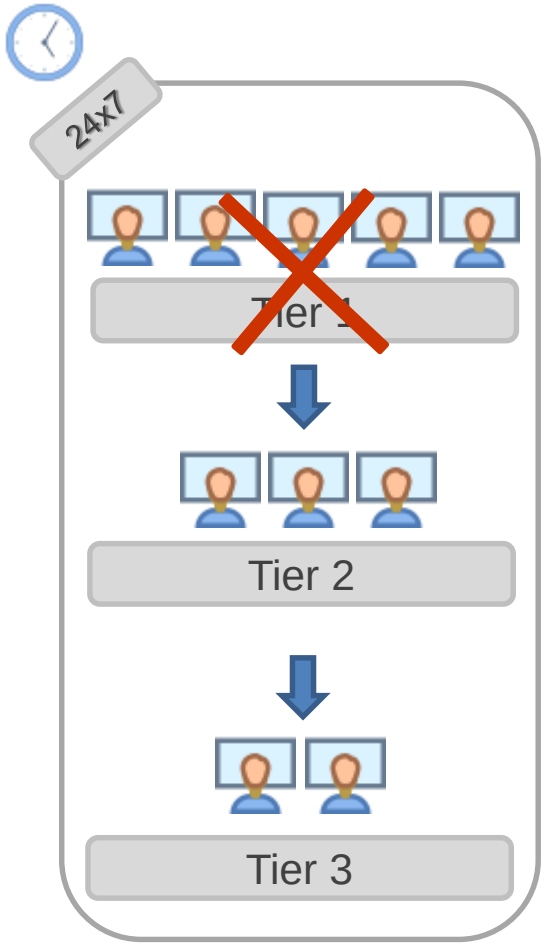
СИСТЕМНЫЙ ОПЕРАТОР
ЕДИНОЙ ЭНЕРГЕТИЧЕСКОЙ СИСТЕМЫ

# SOC это скучно…

**или**
**(лучший отдых — это смена деятельности)**

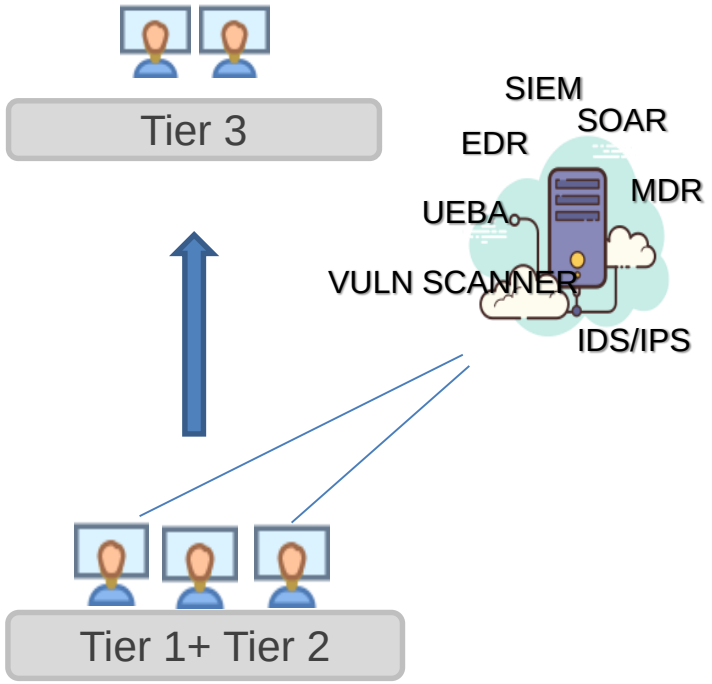
# Классическая структура SOC и ее минусы




- Первая линия SOC малоэффективна, из-за малого набора необходимых компетенций и человеческого фактора
- Ограниченный функционал, который может быть реализован средствами автоматизации
- Увеличивается время цикла обработки события ИБ
- Более высокие траты на содержание SOC

# О нашем SOC




- Обработка порядка 1 000 000 000 событий за сутки, по результату которой создается до **30** кейсов в сутки.

- Специалисты третьего уровня участвовали в разборе 4-х % кейсов за 2018 год

- Среднее время обработки кейса за 2018 год составило 7,5 часов

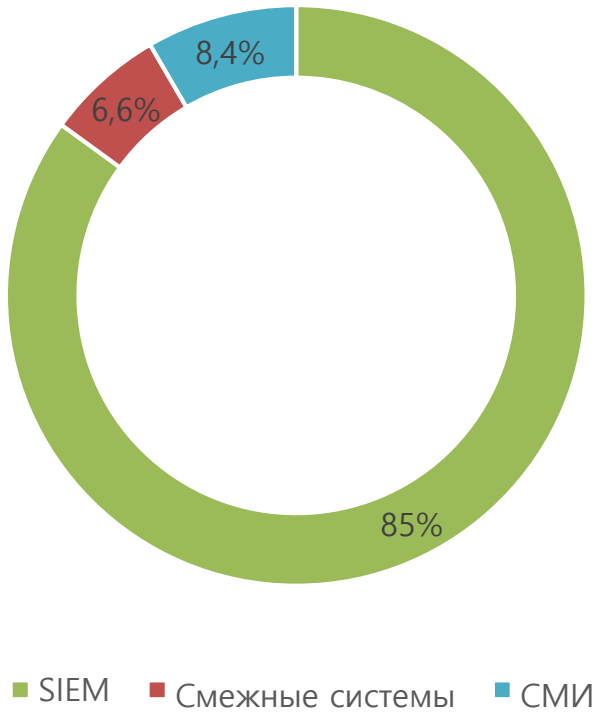
# Предполагаемое распределение времени в среднестатистическом SOC

| | |
|---|---|
| SIEM | 70% |
| Смежные системы | 20% |
| СМИ | 10% |


| | |
|---|---|
| 20% | SIEM |
| 40% | Смежные системы |
| 40% | СМИ |

*«90 процентов средняя ротация аналитиков первой линии в Европе и Соединенных Штатах Америки» – Алексей Лукацкий.*

# Хронометраж времени работника SOC «СО ЕЭС»




- Малый процент (6,6 %) времени проводимого работником в смежных системах, обусловлен интеграцией большинства данных систем с SIEM.

- В настоящее время подключено к SIEM 5834 источника.

# Дополнительные проекты

Определяются ответственные за проект, контрольные точки (промежуточные результаты) и конечный желаемый результат

Совместное обсуждение дополнительных проектов


Не более 20 % рабочего времени на дополнительный проект

Необходимо детализировать дополнительный проект

*Формула дополнительных проектов = Закон Парето помноженный на эффект Сеченова*

# Реализованные проекты

- Комплексное тестирование open source Firewall решений, по результату подготовлен отчет о работе интересующего нас функционала в тестируемых решениях.

- Проработка задачи по документальному оформлению сегментации сети, в результате профильные службы начали реализацию изменений.

- Тестирование функционала active response на наших IDS, итоги тестирования использованы в новой архитектуре системы защиты.

# О чем не стоит забывать?

СИСТЕМНЫЙ ОПЕРАТОР
ЕДИНОЙ ЭНЕРГЕТИЧЕСКОЙ СИСТЕМЫ

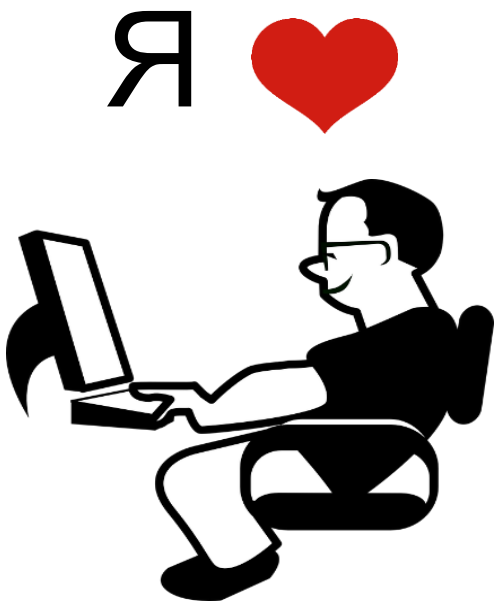
- Проекты «дополнительные» и у работника присутствует основной функционал, который он должен выполнять. Всегда должен быть баланс между выполнением основных обязанностей и решением задач в рамках дополнительного проекта.

- Среди дополнительных проектов не должно быть критичных проектов с фиксированным сроком исполнения.

- Сотрудник должен иметь выбор (должна быть возможность подобрать проект «под себя»).

- Также не стоит забывать, что «любой успешный результат должен оплачиваться», т.е. должна быть продумана система мотивации.

# В чем плюсы данной активности ?




- Позволяет не погрязнуть в рутине
- Возможность побывать в новой роли и реализовать/повысить свои компетенции, которые не востребованы в типичной для 1-2 линии SOC деятельности
- Помимо рутинной работы, появляется и работа с конкретным лично созданным результатом

СИСТЕМНЫЙ ОПЕРАТОР
ЕДИНОЙ ЭНЕРГЕТИЧЕСКОЙ СИСТЕМЫ

**Спасибо за внимание!**