Система мониторинга ИБ промышленного предприятия. Опыт создания.

Н.А. Домуховский

Заместитель генерального директора

УЦСБ ИНТЕГРАТОР СИЛЬНЫХ РЕШЕНИЙ

Немного о нас...

Мониторинг безопасности – что это?

Мониторинг – процесс сбора информации с целью наблюдений, оценки и прогноза изменений состояния объекта

Безопасность – состояние защищенности …

Мониторинг безопасности – что это?

Мониторинг – процесс сбора информации с целью наблюдений, оценки и прогноза изменений состояния объекта

Безопасность – состояние защищенности …

Мониторинг безопасности – что это?

Мониторинг – процесс сбора информации с целью наблюдений, оценки и прогноза изменений состояния объекта

Безопасность – состояние защищенности ...

как мерить?

чем мерить?

что делать с результатом?

Мониторинг безопасности – зачем это?

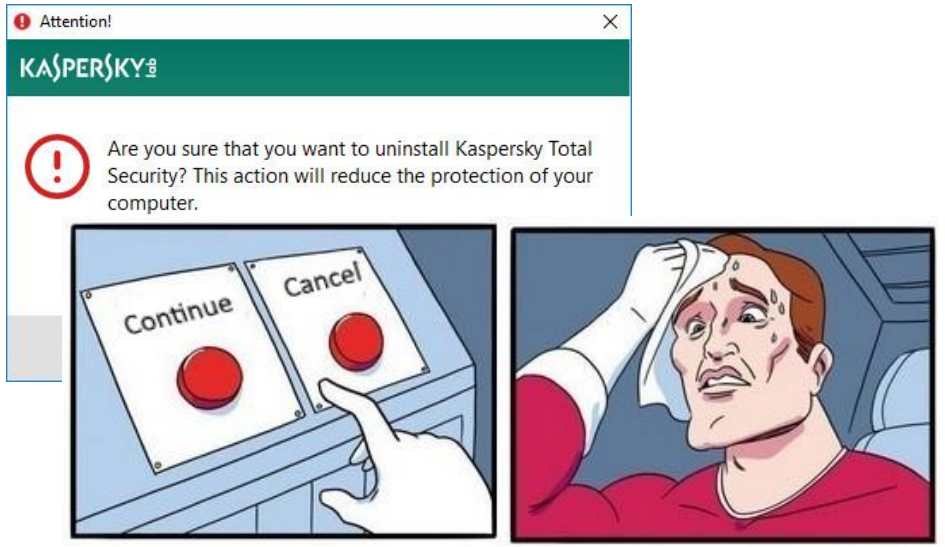
USSC

Соответствие требованиям регулирующих органов по обеспечению безопасности ОКИИ, АСУ КВО и пр.

Своевременное выявление деградации системы обеспечения ИБ и принятие корректирующих мер

Выявление инцидентов ИБ, которые могут произойти и в защищенной системе

АУД.7	Мониторинг безопасности



Метод мониторинга безопасности АСУ ТП

Доверенная система

- Контроль целостности ПО и конфигурации (программной и аппаратной)
- Контроль информационных потоков
- Отсутствие инструментов внесения изменений (в том числе, в конфигурации)

Контролируемый канал связи

Смежная система

Непрерывный мониторинг отклонений

Метод мониторинга безопасности АСУ ТП

Защищаемая система

- Контроль целостности ПО и конфигурации (программной и аппаратной)
- Контроль информационных потоков
- Отсутствие инструментов внесения изменений (в том числе, в конфигурации)

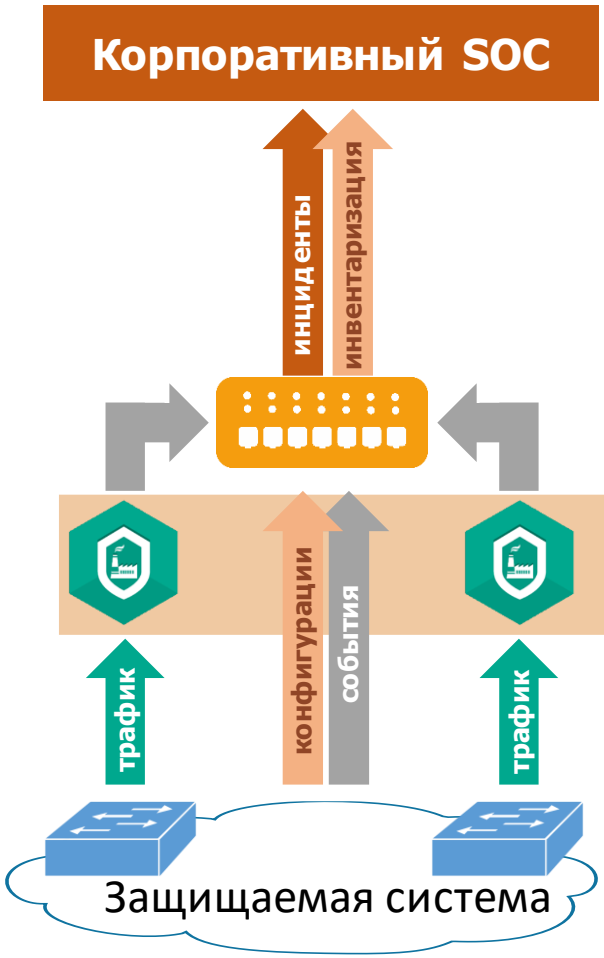
Контролируемый канал связи

Смежная система

Непрерывный мониторинг отклонений

Модель – это упрощение действительности. Поэтому, кроме перечисленного, необходимо осуществлять сбор и анализ событий безопасности со всех компонентов системы

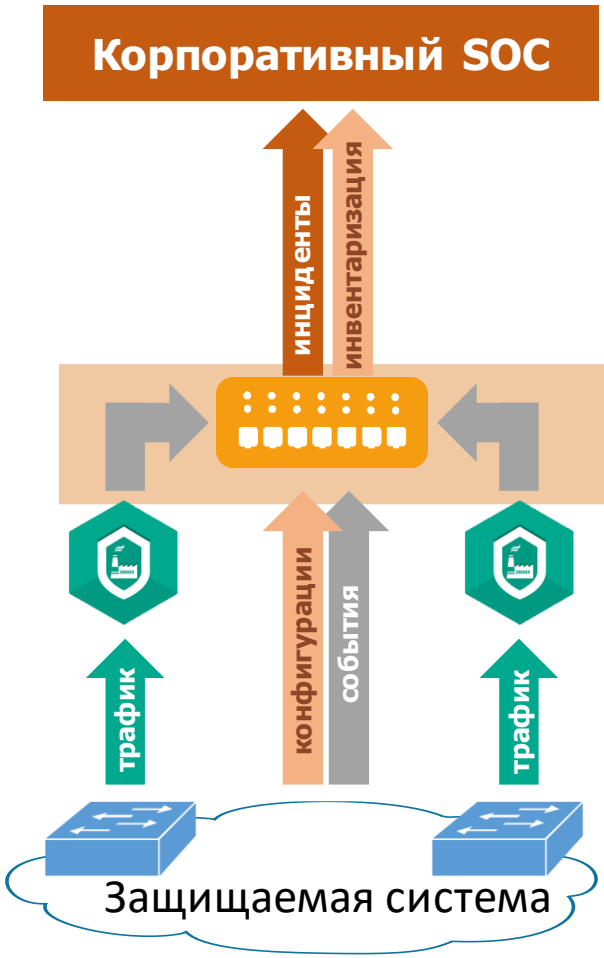
Архитектура системы мониторинга безопасности АСУ ТП



KICS for Networks обеспечивает:

- обнаружение аномалий и атак в промышленной сети

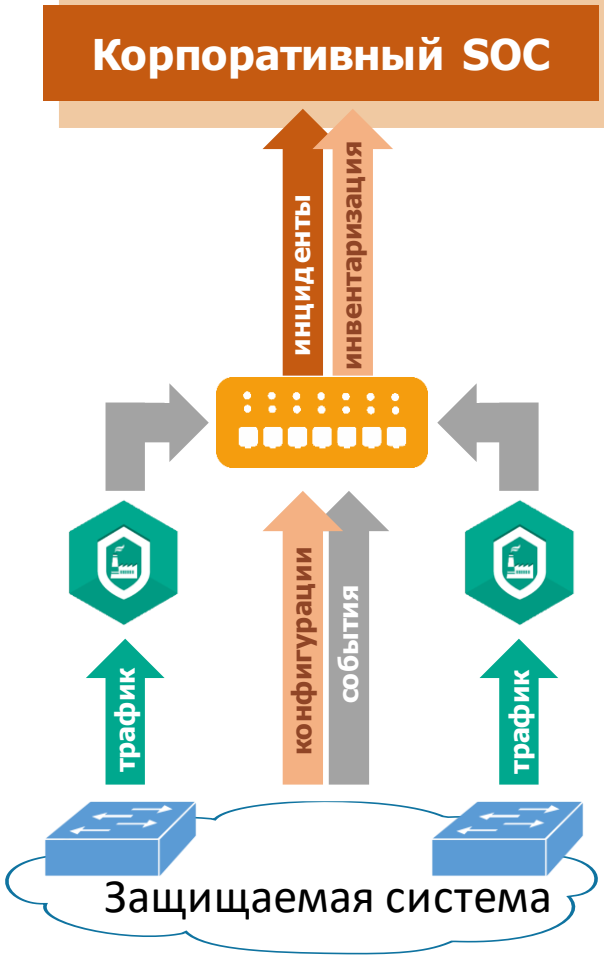
Архитектура системы мониторинга безопасности АСУ ТП



DATAPK обеспечивает:

- сбор событий ИБ с объектов промышленной сети
- инвентаризация объектов промышленной сети и их конфигураций
- анализ событий ИБ
- интеграция с корпоративным SOC

Архитектура системы мониторинга безопасности АСУ ТП



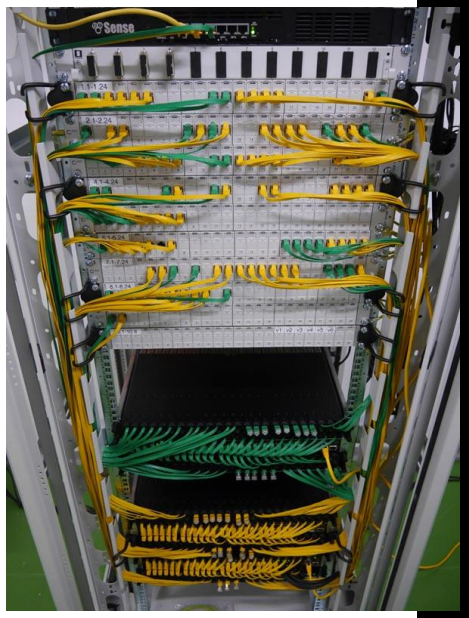
Корпоративный SOC обеспечивает:

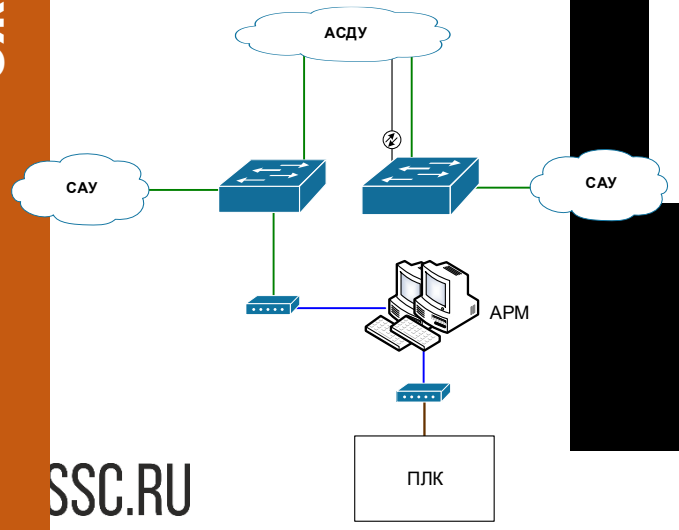
- систематизацию и визуализацию событий ИБ
- обогащение событий ИБ данными инвентаризации
- автоматизацию процесса управлениями инцидентами ИБ

Объект мониторинга. Ожидание vs реальность

USSC

Ожидание





Не используется STP?

Нет свободных портов?

Полно неуправляемых коммутаторов?

Схемы нет или неактуальная?

Кольцо?

Никто не знает, где расположено оборудование?

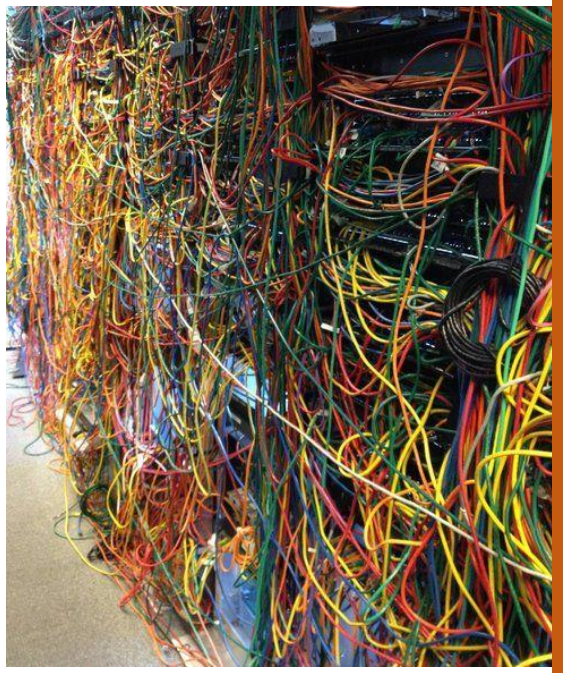
Плоская сеть?

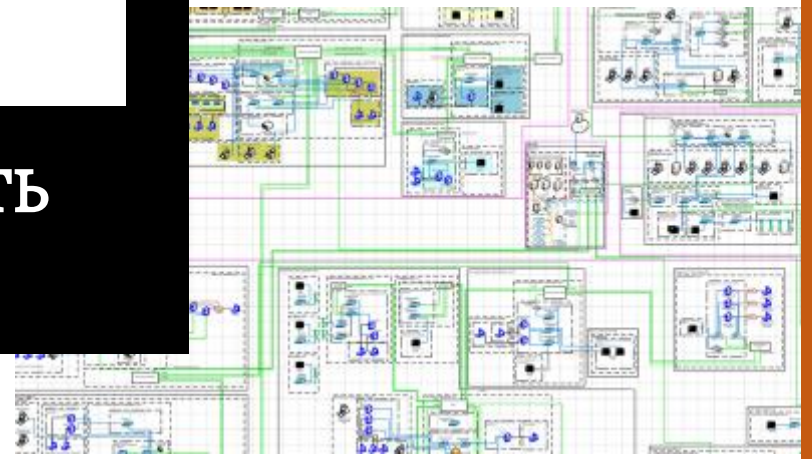
Кольцо в кольце?

Пароль к коммутатору утерян давным-давно?

Не знают про Cisco Hierarchical Network Design?

Когда начал обследовать промышленную сеть





Реальность

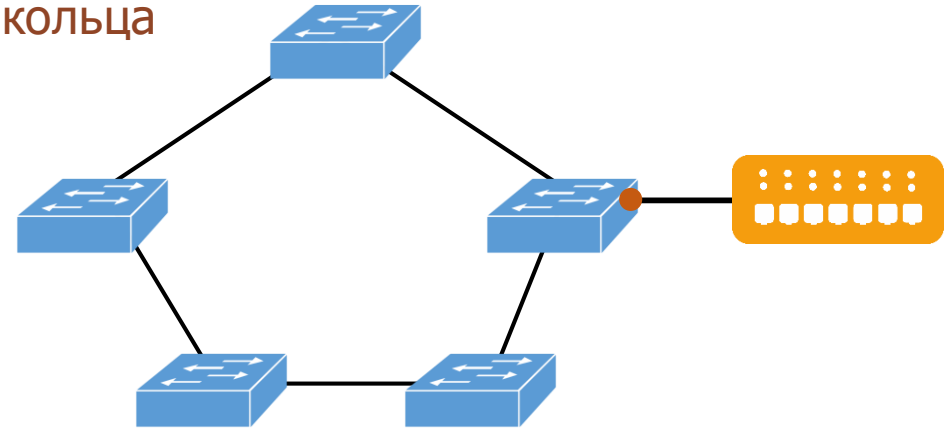
Построение сети мониторинга

Вариант построения	Плюсы	Минусы
Модернизация сети АСУ ТП	• 100%-я видимость сети • Более управляемая и надежная сеть	• Дорого • Долго • Может потребоваться согласование проектировщиков АСУ ТП
Отдельная сеть мониторинга	• Нет дополнительной нагрузки на технологическую сеть • Быстрее и дешевле модернизации	• Могут потребоваться дополнительные физические каналы связи • Требуется портовая емкость на АСО АСУ ТП
Увеличение числа сенсоров	• Отсутствие влияния на сеть АСУ ТП • Можно задействовать существующее оборудование	• Требуется портовая емкость на АСО АСУ ТП • Дополнительные затраты на лицензии ПО мониторинга сети

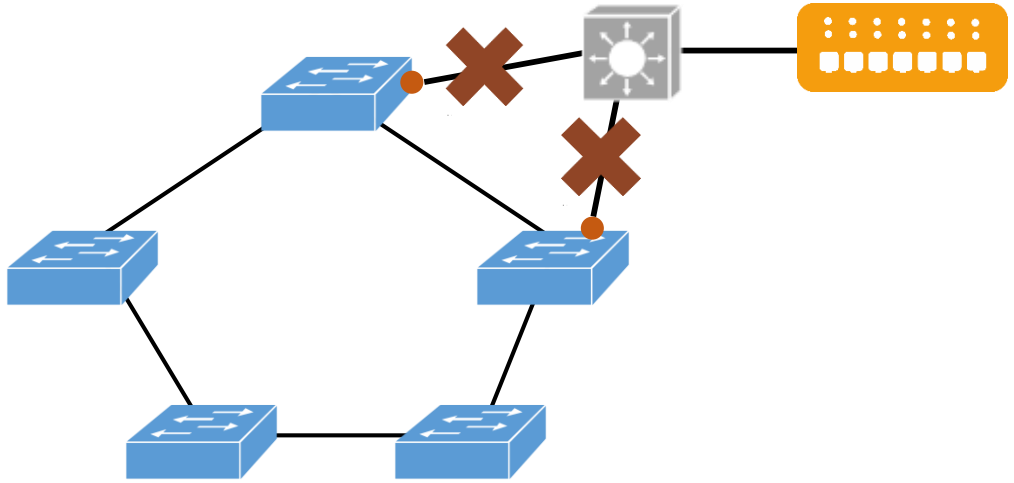
Стоит отказаться от мечты анализировать 100% трафика технологической сети

Сеть мониторинга. Tips & Tricks

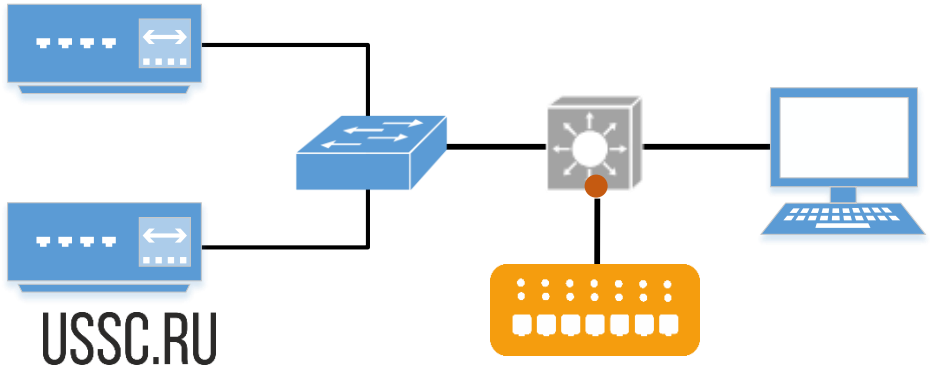
Трафик кольца может быть снят через любой коммутатор кольца



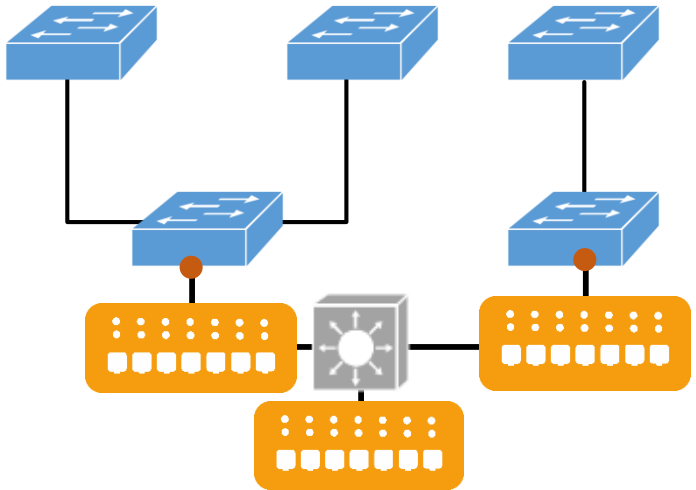
Не рассчитывать на STP!



Если 100% трафика не получить – выбирать точку съема с основными информационными потоками

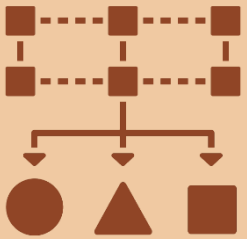


Строить независимую сеть мониторинга



Обработка данных мониторинга безопасности

Приоритизация:
- учет критичности события, объекта, системы и пр.
- показывать только то, что требует понятной реакции оператора
- разделение данных по времени («свежие» и «несвежие» инциденты)



Классификация:
- по источникам (производство, АСУ ТП, объект АСУ ТП)
- по типам (инцидент, тревога, информационное сообщение)
- по временным отрезкам (оперативные, архивные)
- …

Обогащение:
- добавление данных инвентаризации от различных источников
- расшифровка служебных полей событий
- добавление структур данных для оперативной работы (карточка инцидента и пр.)

Обработка данных мониторинга безопасности

Эксплуатационный мониторинг DATAPK средний уровень	Эксплуатационный мониторинг DATAPK базовый уровень	Эксплуатационный мониторинг KICS
21	33	10

Активные ОЗ за все время	Активные ОЗ за последние 24 часа	Активное АСО за все время	Активное АСО за последние 24 часа	Активные Windows за все время	Активные Windows за 24 ч	Активные Linux за все время	Активные Linux за последние 24 часа
866	658	229	173	669	517	8	4

Информационные

Предприятие	Изменение АСУ	Изменение ОЗ	В/А	Н/Д	Сбой ОЗ	Предупреждение
[redacted]	0	14	3	0	0	3
[redacted]	0	0	12	0	0	2
[redacted]	0	53	24	33	0	8
[redacted]	17	95	19	13	16	12
[redacted]	5	286	33	0	13	9

Из чего собрать SOC?

ГосСОПКА

Сведения о компьютерных инцидентах

CMDB, ИТ-мониторинг

Сведения о ИТ-активах

Система автоматизации процессов управления ИБ

- Инвентаризация информационных ресурсов
- Автоматизация категорирования ОКИИ
- Автоматизация анализа угроз ИБ
- Автоматизация управления инцидентами ИБ
- …

Автоматизация бизнес-процессов

BPM, СЭД

- **сведения об объектах защиты**
- **уязвимостях**
- **инцидентах**

Система обеспечения ИБ

Система мониторинга. Ключевые факторы успеха

USSC

1. **Не оставлять белых пятен в плане**
   Сразу определите кто и как будет наводить порядок в промышленной сети
2. **Обеспечить безопасность объекта мониторинга**
   Не забудьте о настройке параметров безопасности объектов промышленной сети
3. **Keep it simple stupid**
   Не надо внедрять высокие технологии в промышленную сеть
4. **80:20**
   Не надо стремиться анализировать 100% трафика (по крайней мере сразу)
5. **Думать о SOCe**
   Что будет выступать в роли SOC и кто будет им пользоваться?

USSC

СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

Николай Домуховский

Заместитель генерального директора

ООО «УЦСБ»
620100, Екатеринбург, ул. Ткачей, д.6
Тел.: +7 (343) 379-98-34
Факс: +7 (343) 382-05-63
info@ussc.ru
www.USSC.ru

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ | USSC.RU