Опыт практической реализации

Начало - ТЗ

Состав систем обеспечения информационной безопасности:

1. Сервис антивирусной защиты;
2. Сервис защиты от несанкционированного доступа и доверенной загрузки;
3. Сервис защиты виртуальной среды;
4. Сервис обеспечения межсетевого экранирования и обнаружению, и предотвращению компьютерных атак;
5. Сервис обеспечения аудита и контроля защищенности;
6. Сервис управления событиями безопасности и реагированию на инциденты;
7. Сервис криптографической защите информации;
8. Сервис подключения к ГосСОПКА;
9. Сервис Центра обеспечения безопасности.

Зачем всё это ?

Для любых ИС является критичными сохранение свойств информации – доступность, целостность, конфиденциальность – или любая их комбинация в зависимости от риск-ориентированной модели управления этой информацией. Применение Сервиса управления событиями безопасности и реагирования на инциденты позволяет контролировать эти свойства информации в ИС и обеспечить:

- **Снижение рисков ИБ за счет своевременного обнаружения и обработки инцидентов в ИС**
- **Повышение уровня управления средствами безопасности и защищенности ИС**
- **Формирование отчетов об инцидентах ИБ в ИС для их последующей передачи в ГосСОПКА**
- **Возможность аудита информационно-телекоммуникационной составляющей ИС и контроля уровня ее защищенности**

управление проектом

«Эскиз» - цели:

Подготовка данных об угрозах для корреляции их с возможными событиями ИБ и определения Профиля событий/инцидентов.

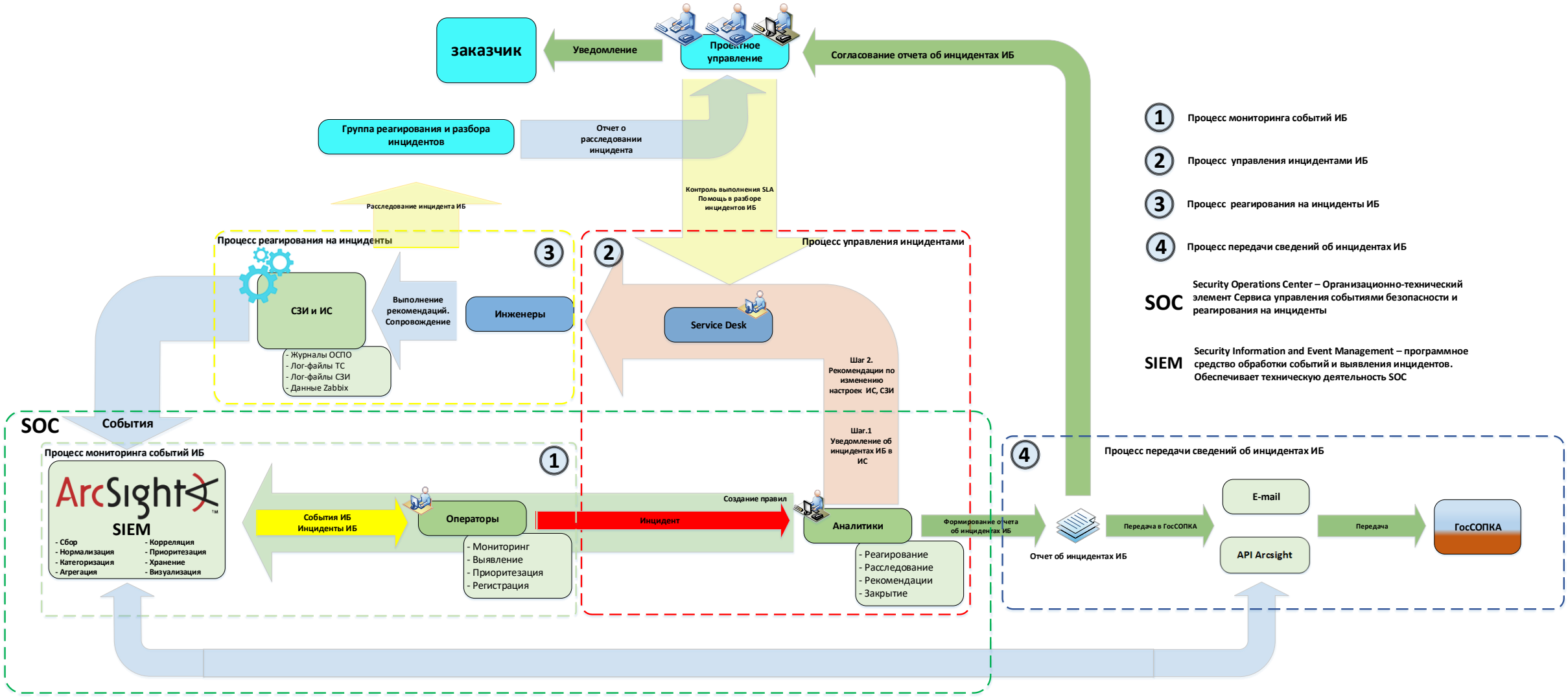
Формирование профиля ключевых элементов ИТ-инфраструктуры.

Определения требований к сервису мониторинга событий безопасности и реагирования на инциденты.

Формирование требований к сервису мониторинга событий безопасности и реагирования на инциденты: требования к SOC; SIEM; Service Desk; к Подсистеме криптографической защиты информации.

Интеграция сервиса мониторинга событий безопасности и реагирования на инциденты в ИТ-инфраструктуру и процессы реагирования на инциденты ИБ: Описание сервиса; Регламент взаимодействия ИТ и ИБ служб владельца ИС и SOC; Регламент технической поддержки; Инструкция по реагированию на инциденты ИБ; Инструкция по ликвидации последствий ИБ.

Регламентация процесса передачи сведений об инцидентах ИБ. Формирование процесса реагирования и ликвидацию последствий компьютерных атак : Разработка соответствующих Инструкций по мониторингу и реагированию на компьютерные атаки; Паспортизация объекта информатизации; Разработка плана тренировок по реагированию на инциденты ИБ.


заказчик
Уведомление
Проектное управление
Согласование отчета об инцидентах ИБ
Группа реагирования и разбора инцидентов
Отчет о расследовании инцидента
Контроль выполнения SLA
Помощь в разборе инцидентов ИБ
Расследование инцидента ИБ
Процесс реагирования на инциденты
3
СЗИ и ИС
- Журналы ОСПО
- Лог-файлы ТС
- Лог-файлы СЗИ
- Данные Zabbix
Выполнение рекомендаций. Сопровождение
Инженеры
2
Процесс управления инцидентами
Service Desk
Шаг 2. Рекомендации по изменению настроек ИС, СЗИ
Шаг.1 Уведомление об инцидентах ИБ в ИС
SOC
События
Процесс мониторинга событий ИБ
1
ArcSight
SIEM
- Сбор
- Нормализация
- Категоризация
- Агрегация
- Корреляция
- Приоритезация
- Хранение
- Визуализация
События ИБ
Инциденты ИБ
Операторы
- Мониторинг
- Выявление
- Приоритезация
- Регистрация
Создание правил
Инцидент
Аналитики
- Реагирование
- Расследование
- Рекомендации
- Закрытие
Формирование отчета об инцидентах ИБ
4
Процесс передачи сведений об инцидентах ИБ
Отчет об инцидентах ИБ
Передача в ГосСОПКА
E-mail
API Arcsight
Передача
ГосСОПКА
1 Процесс мониторинга событий ИБ
2 Процесс управления инцидентами ИБ
3 Процесс реагирования на инциденты ИБ
4 Процесс передачи сведений об инцидентах ИБ
SOC Security Operations Center – Организационно-технический элемент Сервиса управления событиями безопасности и реагирования на инциденты
SIEM Security Information and Event Management – программное средство обработки событий и выявления инцидентов. Обеспечивает техническую деятельность SOC

перечень сведений об инцидентах ИБ

№	Наименование типа отчетного инцидента	Предоставляемая информация
1	Вредоносное ПО	Внутренний IP-адрес ЭВМ; Внешний IP-адрес ЭВМ; Имя зараженного устройства; Известные сведения о бот-сети; Доменное имя, IP-адрес или URL ЦУ; Классификация ВПО; Контрольная сумма выявленного образца ВПО; Образец ВПО ; Адреса электронных почтовых ящиков с которых поступило письмо с вложением; Имя файла с исходным кодом электронного письма; URL вредоносного ресурса с которого было загружено ВПО; Перехваченные команды управления
2	Эксплуатация уязвимостей	IP-адрес пострадавшей ЭВМ; Имя пострадавшего устройства; Тип ЭВМ; URL или IP-адрес источника атаки; Тип уязвимости; Последствия эксплуатации уязвимости
4	DoS/DDoS	Доменное имя, IP-адрес или подсеть пострадавшего объекта; Источники атаки; Тип атаки; Мощность атаки; Время начала атаки; Время окончания атаки
5	Перебор паролей	IP-адрес пострадавшего объекта; Имя пострадавшего устройства; Источники атаки; Тип атаки; Мощность атаки; Какая учетная запись была скомпрометирована
6	ЦУ бот-сети	URL и IP-адрес пострадавшей системы; Имя пострадавшего устройства; Известные сведения о бот-сети
7	Вредоносный ресурс	URL и IP-адрес пострадавшей системы; Имя пострадавшего устройства; Тип вредоносной активности
8	Запрещенный контент	URL и IP-адрес пострадавшей системы; Имя пострадавшего устройства; Тип контента
9	Неавторизованный доступ	Типы контента
10	Сканирование ресурсов	Информация о атакующих адресах/хосте; Информация о атакуемом адресе/хосте; Метод сканирования; Сканируемые порты, сигнатуры

то, что интересует всех, а некоторых даже и волнует

С чего начать, чем продолжить и вообще с какого края разматывать – только практический опыт;

«помощники» - уважаемые компании в части помощи как SOC – только практический опыт;

ArcSight & Qradar & MaxPatrol SIEM – кому как нравится :) , но не до «игровых эксперементов»;

по опыту, хорошо может получиться и вовсе без SIEM (почему – см. презентацию А. Новикова)