ИНФОСИСТЕМЫ ДЖЕТ

Как запустить конвейер. Выстраивание архитектуры и процессов SOC

Андрей Янкин,
руководитель отдела консалтинга ИБ

Security Operation Center

SOC (Security Operation Center) – это команда, организованная для обнаружения, анализа, реагирования, уведомления и предотвращения инцидентов информационной безопасности.

Эффективный SOC = персонал + процессы + технические инструменты

SOC: функции

Обработка данных в реальном времени

- **Колл-центр**
- Мониторинг и разбор данных в режиме реального времени

Работа с внешними источниками информации, стратегическое планирование

- Сбор внешних данных и их анализ
- Распространение информации из внешних источников
- Подготовка материалов для внешнего распространения
- Обогащение правил SOC на основе внешних данных
- Стратегическое планирование
- Оценка угроз

Анализ и реагирование на инциденты

- Анализ инцидентов
- Слежка за нарушителем
- Координация реагирования на инциденты
- Внедрение контрмер
- Работы по реагированию на инцидент на пострадавшей площадке
- Удаленное реагирование на инцидент

Анализ цифровых образцов

- Сбор цифровых образцов
- Анализ вредоносного кода
- Анализ прочих цифровых образцов

Обеспечение работоспособности инструментов SOC

- Поддержка работы граничных систем сетевой безопасности
- Поддержка работы инфраструктуры SOC
- Поддержка работы сенсоров
- Создание собственных правил и сигнатур
- Подбор и внедрение решений, использующихся в работе SOC
- Разработка решений, использующихся в работе SOC

Аудит и отслеживание внутренних угроз

- Сбор и хранение данных аудита
- Управление и обработка данных аудита
- Поддержка при работе с внутренними угрозами
- Расследование случаев внутренних нарушений

Сканирование и оценка защищенности

- Создание и актуализация карт сети
- Сканирование уязвимостей
- Оценка защищенности
- Тестирование на проникновение

Прочее

- Оценка средств защиты
- Консультирование по вопросам информационной безопасности
- Повышение осведомленности
- Оперативное информирование
- Распространение наработок
- Взаимодействие с общественностью и СМИ

SOC: использование инструмента SIEM

Обработка данных в реальном времени

- **Колл-центр**
- Мониторинг и разбор данных в режиме реального времени

Работа с внешними источниками информации, стратегическое планирование

- Сбор внешних данных и их анализ
- Распространение информации из внешних источников
- Подготовка материалов для внешнего распространения
- Обогащение правил SOC на основе внешних данных
- Стратегическое планирование
- Оценка угроз

Анализ и реагирование на инциденты

- Анализ инцидентов
- Слежка за нарушителем
- Координация реагирования на инциденты
- Внедрение контрмер
- Работы по реагированию на инцидент на пострадавшей площадке
- Удаленное реагирование на инцидент

Анализ цифровых образцов

- Сбор цифровых образцов
- Анализ вредоносного кода
- Анализ цифровых образцов

Обеспечение работоспособности инструментов SOC

- Поддержка работы граничных систем сетевой безопасности
- Поддержка работы инфраструктуры SOC
- Поддержка работы сенсоров
- Создание собственных правил и сигнатур
- Подбор и внедрение решений, использующихся в работе SOC
- Разработка решений, использующихся в работе SOC

Аудит и отслеживание внутренних угроз

- Сбор и хранение данных аудита
- Управление и обработка данных аудита
- Поддержка при работе с внутренними угрозами
- Расследование случаев внутренних нарушений

Сканирование и оценка защищенности

- Создание и актуализация карт сети
- Сканирование уязвимостей
- Оценка защищенности
- Тестирование на проникновение

Прочее

- Оценка средств защиты
- Консультирование по вопросам информационной безопасности
- Повышение осведомленности
- Оперативное информирование
- Распространение наработок
- Взаимодействие с общественностью и СМИ

Ядровые домены

Outsource VS Insource

Параметр	Insource	Outsource
Контроль	Полный	Частичный
Настройка под себя	Полностью	Стандартные сервисы
Скорость развертывания	До 2 лет	2 месяца
Стоимость	Дешевле через 3-5 лет	Дешевле на старте, OPEX
Качество	???	Предсказуемое

Типовой outsource

Обработка данных в реальном времени

- **Колл-центр**
- Мониторинг и разбор данных в режиме реального времени

Работа с внешними источниками информации, стратегическое планирование

- Сбор внешних данных и их анализ
- Распространение информации из внешних источников
- Подготовка материалов для внешнего распространения
- Обогащение правил SOC на основе внешних данных
- Стратегическое планирование
- Оценка угроз

Анализ и реагирование на инциденты

- Анализ инцидентов
- Слежка за нарушителем
- Координация реагирования на инциденты
- Внедрение контрмер
- Работы по реагированию на инцидент на пострадавшей площадке
- Удаленное реагирование на инцидент

Анализ цифровых образцов

- Сбор цифровых образцов
- Анализ вредоносного кода
- Анализ прочих цифровых образцов

Обеспечение работоспособности инструментов SOC

- Поддержка работы граничных систем сетевой безопасности
- Поддержка работы инфраструктуры SOC
- Поддержка работы сенсоров
- Создание собственных правил и сигнатур
- Подбор и внедрение решений, использующихся в работе SOC
- Разработка решений, использующихся в работе SOC

Аудит и отслеживание внутренних угроз

- Сбор и хранение данных аудита
- Управление и обработка данных аудита
- Поддержка при работе с внутренними угрозами
- Расследование случаев внутренних нарушений

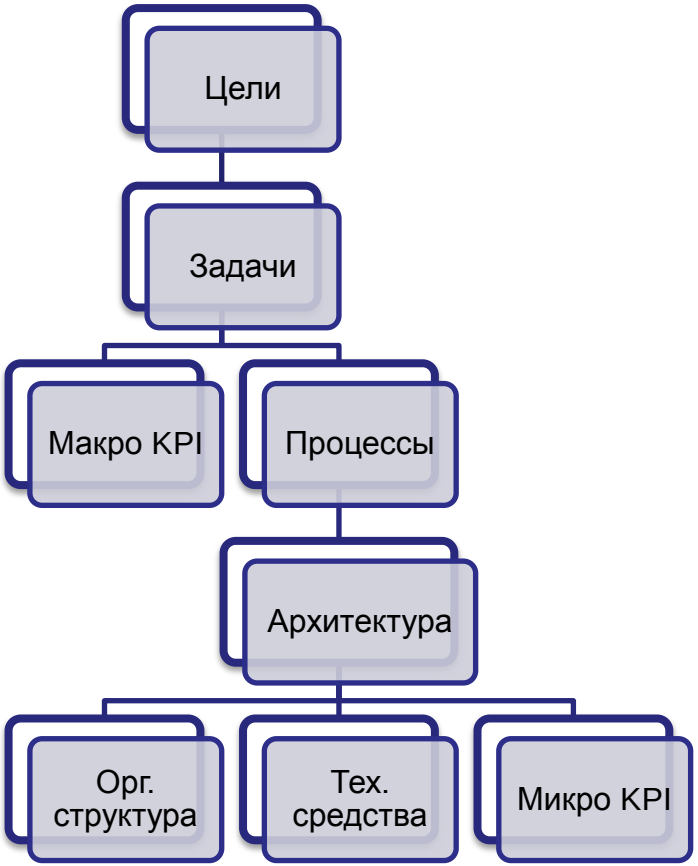
Сканирование и оценка защищенности

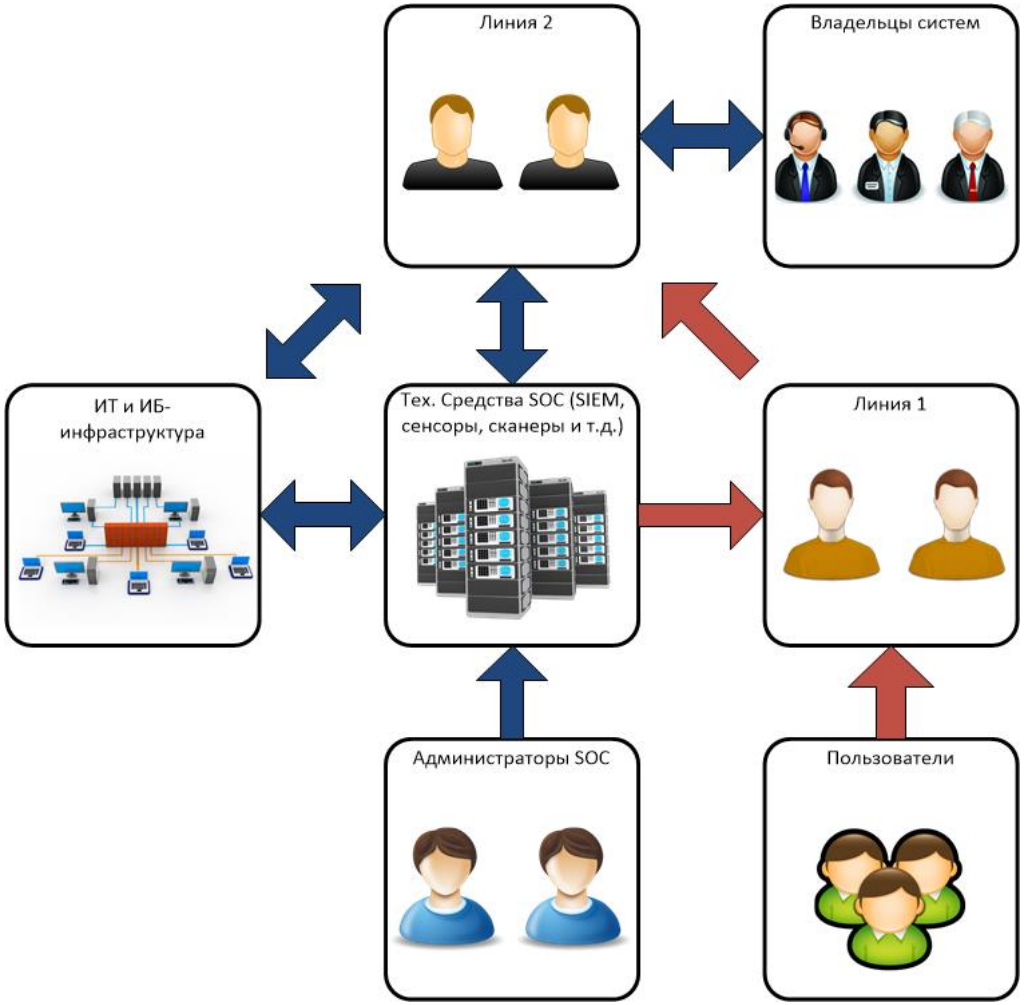
- Создание и актуализация карт сети
- Сканирование уязвимостей
- Оценка защищенности
- Тестирование на проникновение

Прочее

- Оценка средств защиты
- Консультирование по вопросам информационной безопасности
- Повышение осведомленности
- Оперативное информирование
- Распространение наработок
- Взаимодействие с общественностью и СМИ

Архитектура





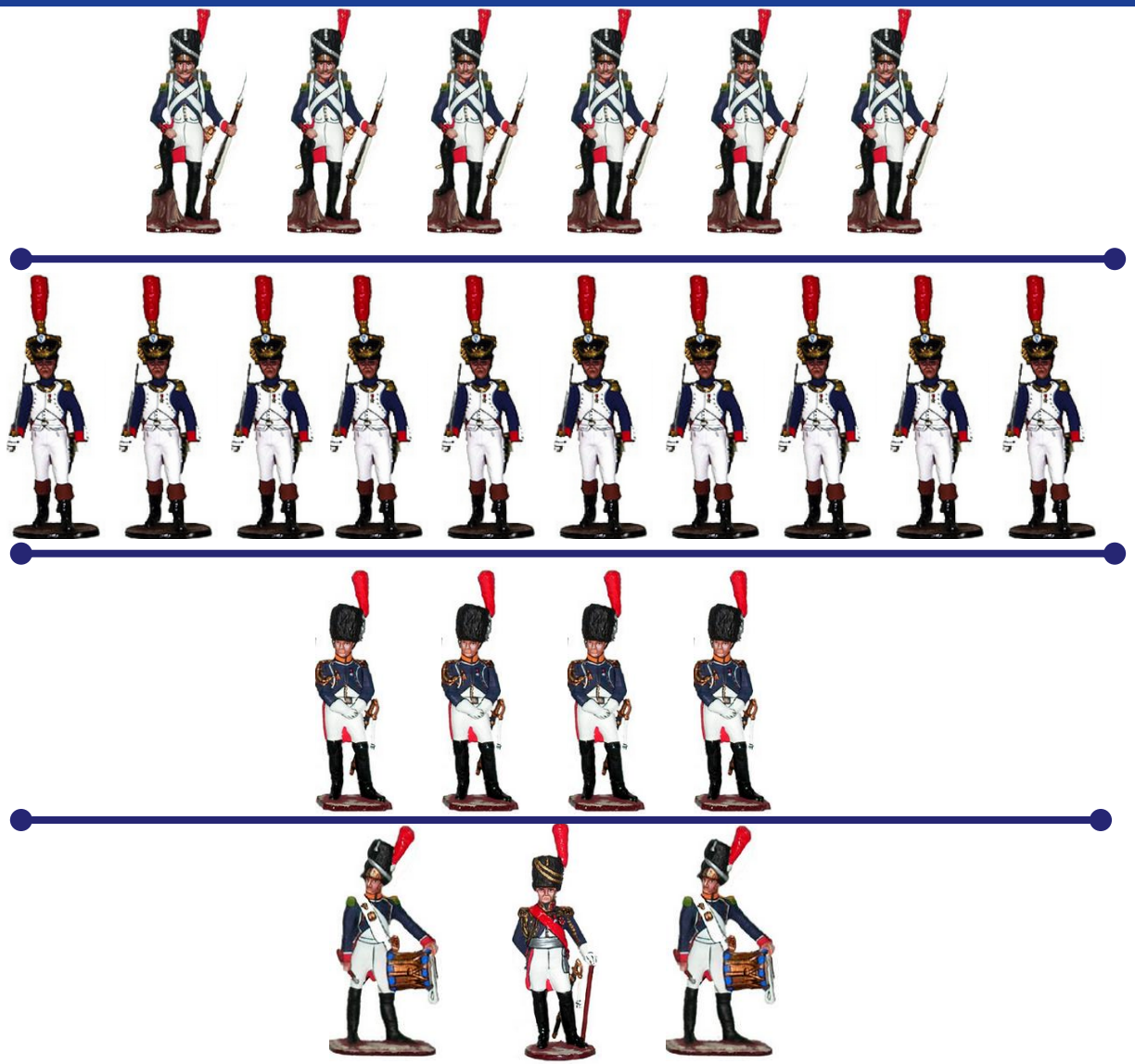
Архитектура

Линия 1

Линия 2

Менеджеры и администраторы

Архитектура



Линия 1

Линия 1,5

Линия 2

Менеджеры и администраторы

Режим работы SOC

- ✓ 24/7 – дорогое удовольствие:
  - Min 8-10 человек на первой линии
  - Min 5 человек на второй линии
  - Сложность найти аналитиков для ночной работы
- ✓ Альтернативные схемы:
  - Смены со смещением по часовым поясам
  - Работа 12/5, 12/7 или 12/5+8/2
  - Вторая линия ночью – на связи

Подбор персонала

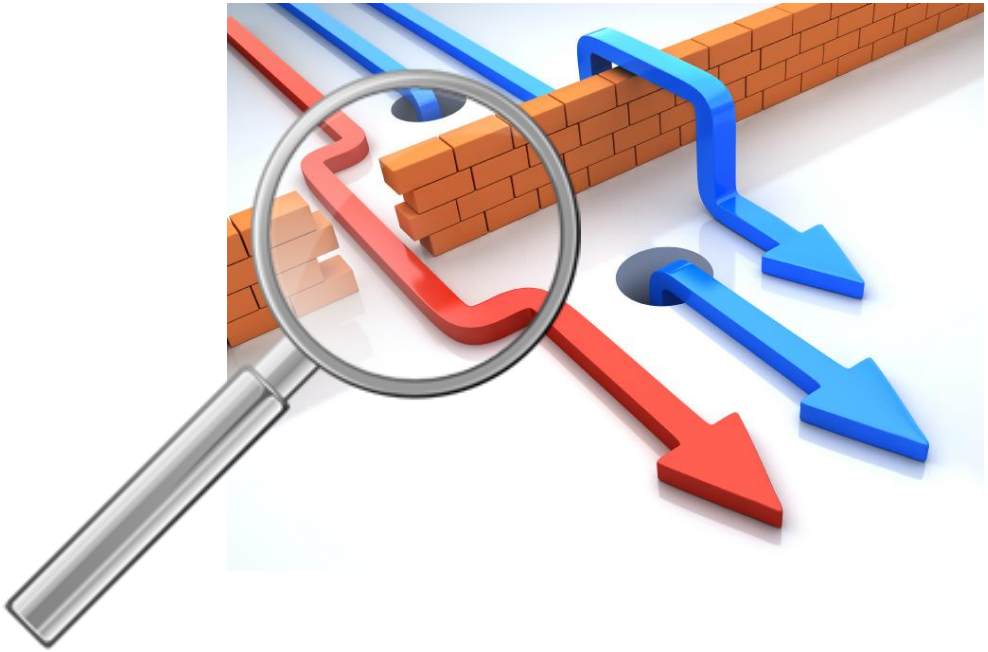
- ✓ Background: администрирование серверов и сети, практическая безопасность (в т.ч. pentest), программирование
- ✓ Работники компании
- ✓ Ядро – звезды
- ✓ Часть ролей – другие подразделения, аутсорсинг

Развитие компетенций

- ✓ Обучение по продуктам
- ✓ Обучение при приеме на работу
- ✓ Регулярный обмен опытом, ротации внутри SOC
- ✓ Анализ, обработка и распространение новостей в области ИБ
- ✓ Обмен опытом с другими SOC, участие в CERT
- ✓ Ясные KPI для сотрудников
- ✓ Обучение не только сотрудников SOC

Имитация нарушений

- ✓ Имитация действий потенциального нарушителя (как внешнего, так и внутреннего)
- ✓ Фиксация реакции средств защиты
- ✓ Рекомендации по настройке средств защиты и обнаружения, SIEM



Информация о контексте работы

SOC

ИТ-инфраструктура

- ИТ-активы
- Сетевая топология
- СЗИ и встроенная безопасность
- Профили штатного функционирования
- Данные об изменениях, статистике
- Уязвимости

Бизнес

- Цели и задачи
- Физическое расположение активов и их ценность
- Взаимоотношения с внешними сторонами, конфликты
- Соответствие между БП и ИС
- Основные группы пользователей, их права и обязанности

Угрозы

- Нарушители
- Векторы атак
- Эксплуатируемые уязвимости

Оперативное информирование

- ✓ SOC – «термометр» ИБ
- ✓ Оперативное информирование руководства, владельцев бизнеса и АС, ИТ-блока, ЭБ, ФБ, департамента рисков, аудиторов и т.д.:
  - Уровень ИБ
  - Риски
  - Угрозы
  - Инциденты
  - Рекомендации
  - Compliance
- ✓ Популяризация SOC

Необходимая документация

Для кого:

- ✓ Руководство
- ✓ Сотрудники SOC
- ✓ Подразделения, задействованные в расследовании инцидентов
- ✓ Аудиторы
- ✓ Все сотрудники компании

Необходимая документация

Уровень	Тип	Примеры
I	Политика верхнего уровня	Политика ИБ
II	Частные политики, стратегии	Политики управления инцидентами ИБ, уязвимостями ИБ, аудитами ИБ, контроля защищенности ИА, обеспечения осведомленности и т.д. Стратегия развития SOC
III	Регламенты	Регламент расследования инцидента ИБ Регламент действий ЮД в случае возникновения инцидента ИБ Регламент оценки эффективности SOC
IV	Операционная документация	Инструкции, формы, журналы, карты сети, обучающие курсы

Выбор технических средств

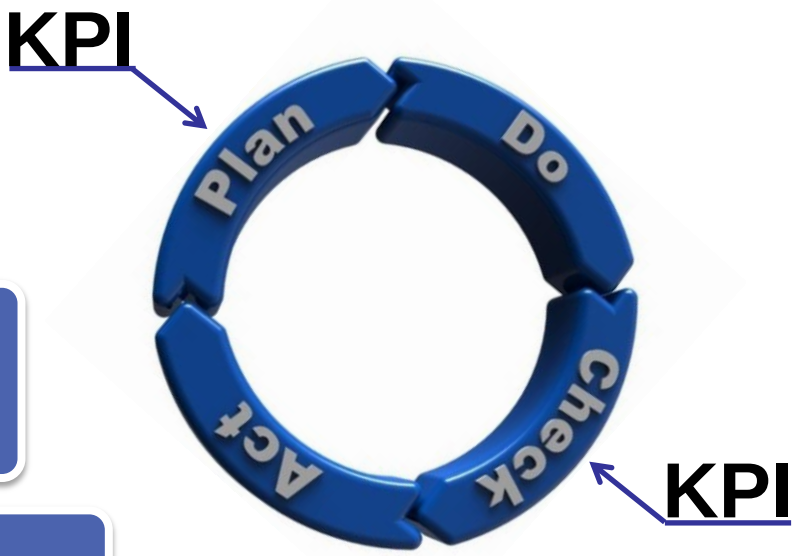
- ✓ SOC – прежде всего команда
- ✓ Тех. средства – инструмент выполнения работы
- ✓ SIEM – центральное ТС SOC, но и оно не обязательно (Log Management + скрипты для маленьких SOC)
- ✓ Инструментов необходимо много:
  - IPS/IDS
  - Сканеры безопасности
  - Service Desk
  - Средства анализа дампов памяти и трафика
  - Инструменты для исследования вредоносов
  - Оснастки для подключения к СУБД, ИС
  - Информационный портал
  - …

KPI

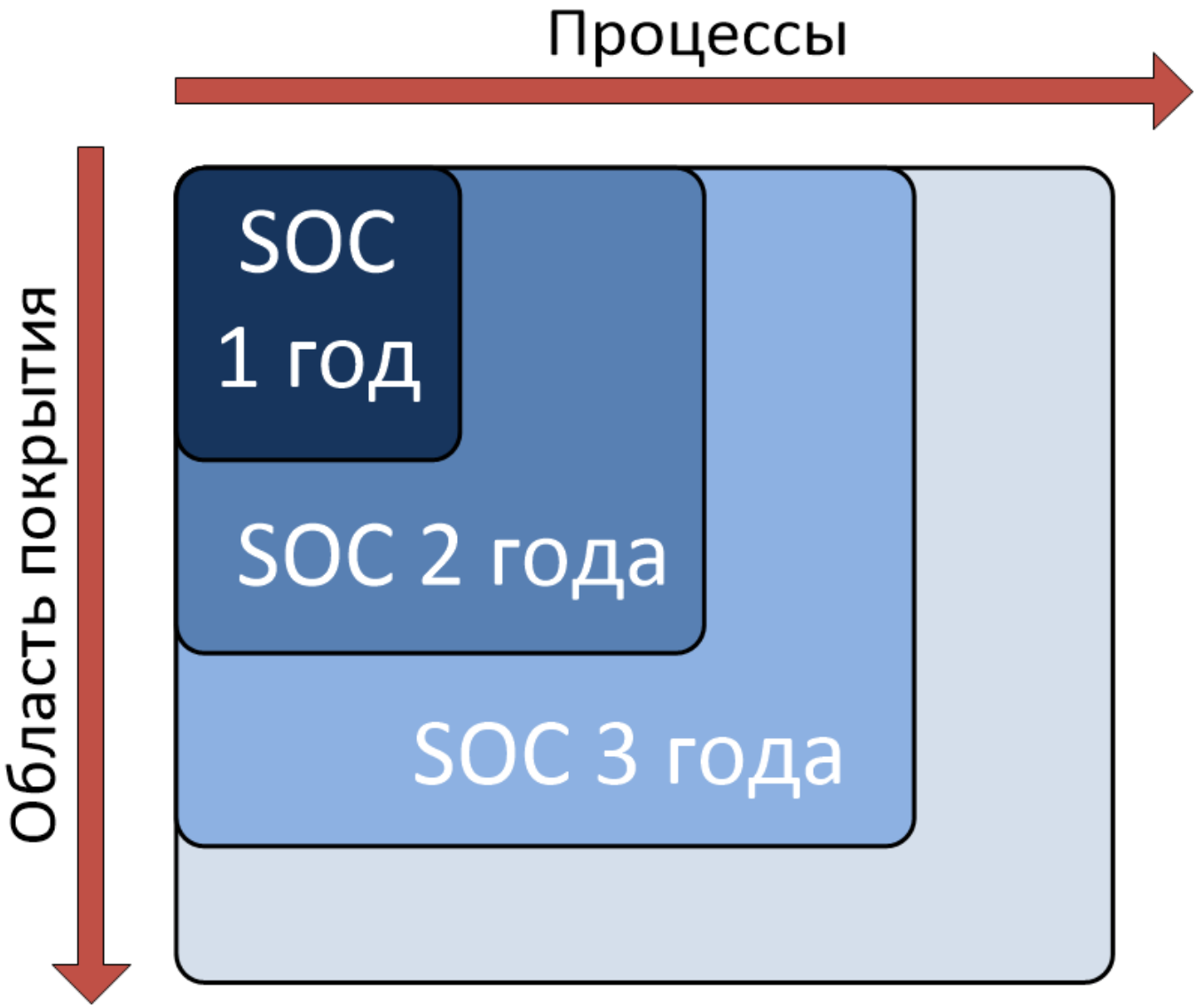
Макро KPI
- Цели и задачи SOC

Микро KPI
- Отдельные процессы

Индивидуальные KPI
- Сотрудники, задания

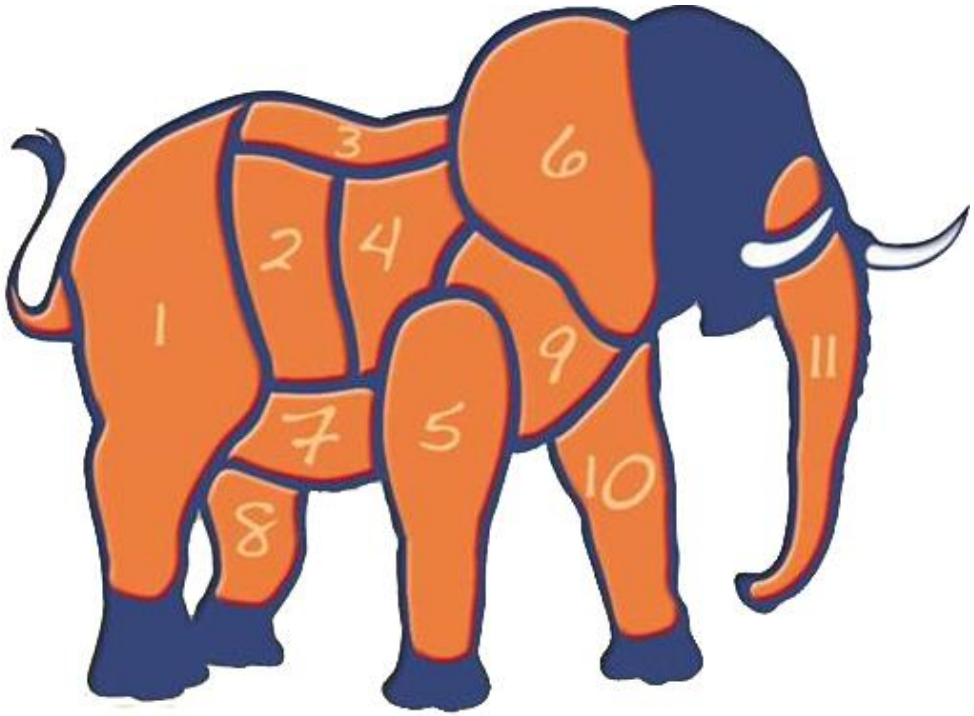


Развитие SOC. Масштабирование



Развитие SOC. Масштабирование

Развивать SOC – как растить слона



SOC 2.0

- ✓ Единый центр реагирования: SOC + ???

- ✓ Банки

- ✓ Промышленность, ТЭК

ИНФОСИСТЕМЫ ДЖЕТ

Контакты:

Андрей Янкин
руководитель отдела консалтинга ИБ
тел: +7 (495) 411-76-01
email: av.yankin@jet.su