Методология создания и работы Security Operation Center (SOC)

Скородумов Анатолий Валентинович

ПАО «Банк Санкт Петербург»

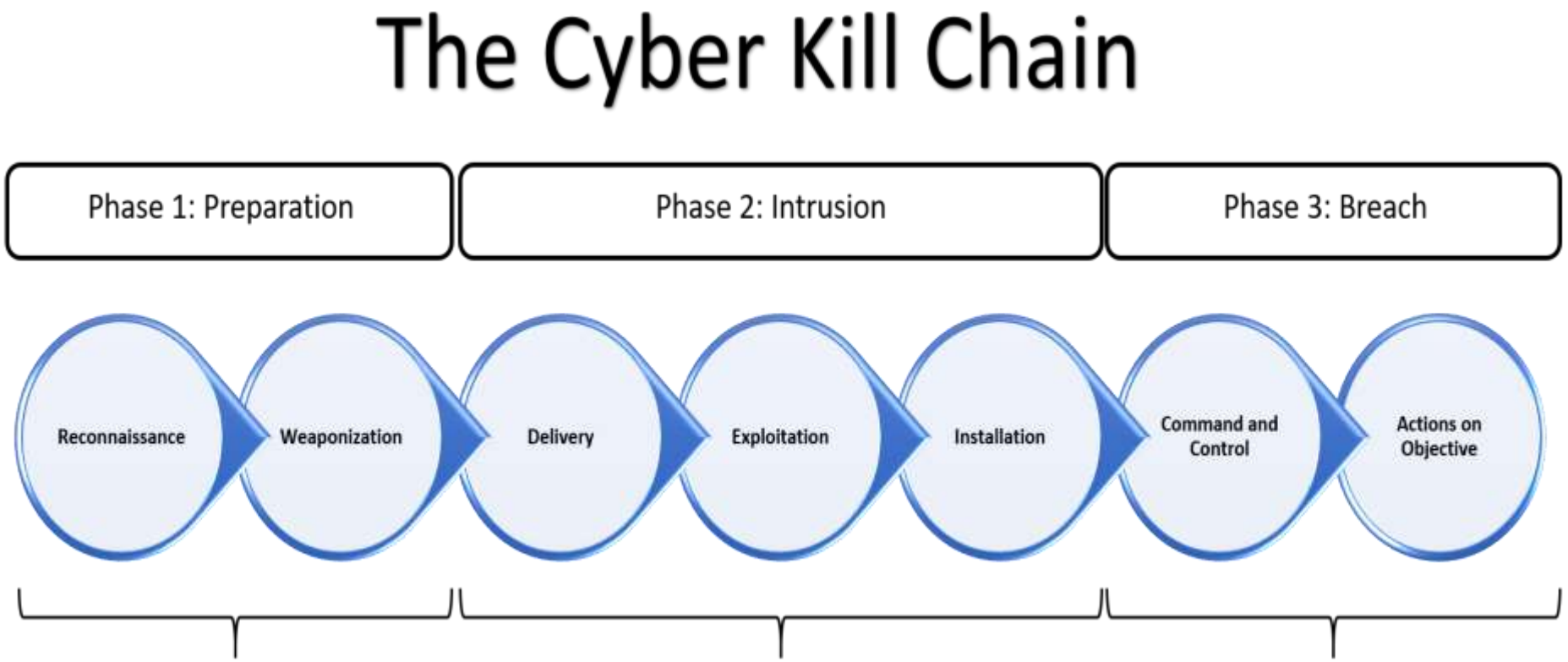
Основные вопросы при создании новой структуры (подразделения)

- **Цель и задачи новой структуры (подразделения)**
- **Основные функции**
- **Определение методологии работы подразделения**

- Положение подразделения в структуре организации
- Организационная структура подразделения
- Требования к кадрам. Решение вопроса по руководителю подразделения
- Определение уровня оплаты сотрудников в данном подразделении
- Порядок набора и обучения персонала
- Размещение подразделения, оборудование рабочих мест

Цели построения SOC

Минимизация возможных потерь за счет раннего выявления и оперативного реагирования на инциденты информационной безопасности



Стандарты и рекомендации по организации работы SOC

- «10 стратегий первоклассного SOC» (Ten Strategies of a World-Class Cybersecurity Operations Center) MITRE
- SANS. «Building a World-Class Security Operations Center: A Roadmap»
- «Концепция совершенствования кибербезопасности критической информационной инфраструктуры» (Framework for Improving Critical Infrastructure Cybersecurity) Национального института стандартов и технологий США (National Institute of Standards and Technology, NIST)
- CIS Controls Центра интернет-безопасности (Center for Internet Security, CIS)
- Стандарты и рекомендации по управлению инцидентами ИБ:
- ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности (ISO/IEC TR 18044:2004 «Information security incident management»)
- РС БР ИББС-2.5-2014 «Менеджмент инцидентов ИБ»
- NIST SP 800-61 «Computer security incident handling guide»
- CMU/SEI-2004-TR-015 «Defining incident management processes for CSIRT»

Основа системы ИБ: люди, процессы, технологии

Люди

лучшие компетенции по ИБ, как внешние , так и внутренние

X

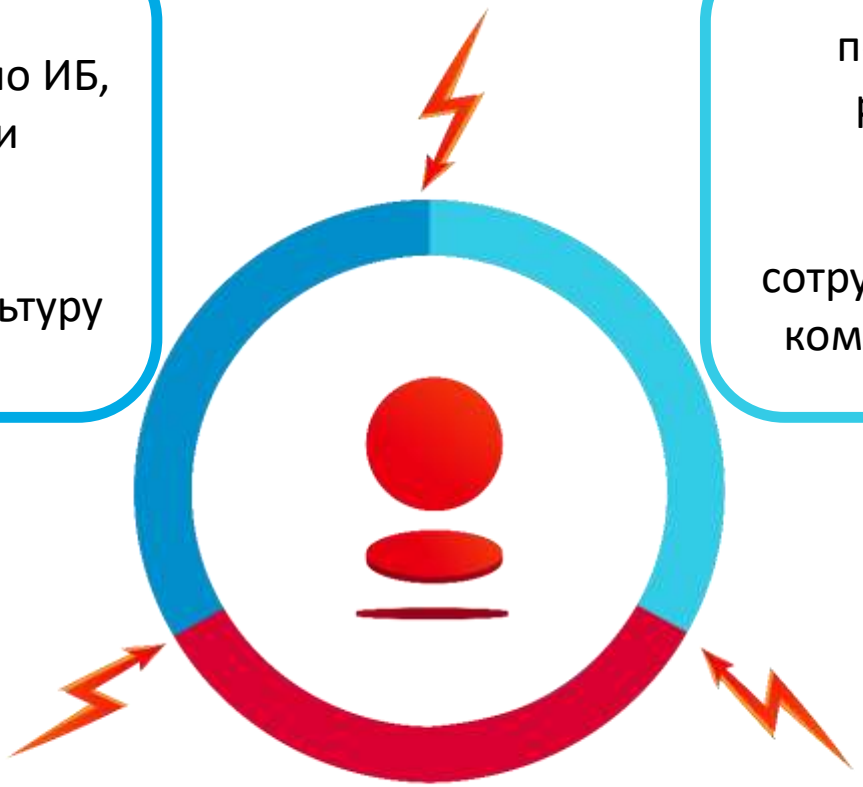
на корпоративную культуру

Технологии

передовые мировые решения в области киберзащиты

+

сотрудничество с ведущими компаниями по защите от киберугроз



Процессы

зрелые процессы и единые стандарты ИБ

+

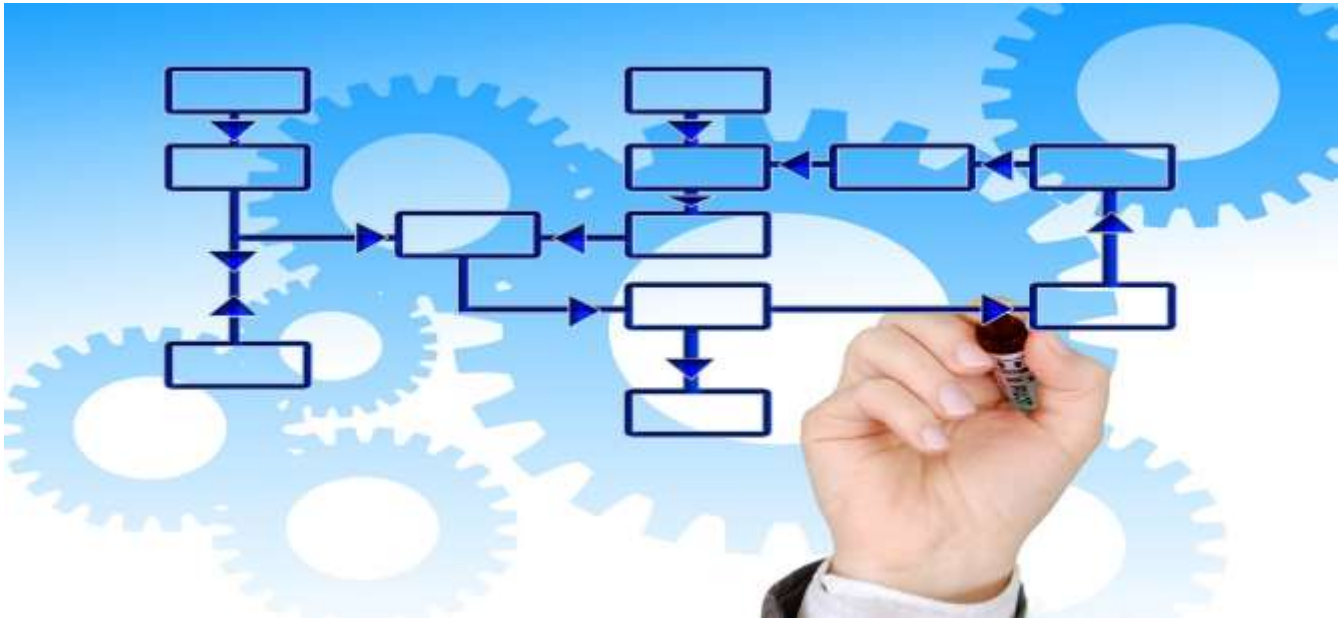
Постоянное совершенствование с учетом вновь появляющихся угроз

Основные процессы SOC

- Мониторинг событий ИБ
- Обработка событий ИБ, их классификация и выявления инцидентов ИБ
- Анализ инцидентов ИБ и сбор дополнительных данных
- Реагирование на инциденты ИБ
- Расследование инцидентов ИБ
- Управление источниками событий ИБ
- Управление уязвимостями
- Взаимодействие со смежными подразделениями
- Сбор и обработка информации о новых угрозах (Threat Intelligence)
- Настройка правил сбора и корреляции событий ИБ
- Ведение базы знаний SOC
- Формирование регулярной отчетности

Перечень связанных процессов

- Управление активами
- Процесс оценки рисков ИБ (формирование моделей нарушителей, моделей угроз с последующей оценкой рисков)
- Управление доступом
- Повышение осведомленности работников в вопросах ИБ
- Процессы управления ИТ изменениями
- Управления ИТ-инцидентами
- Процессы взаимодействия с клиентами



Основные технологии SOC

- Система сбора и корреляции событий (SIEM)
- Автоматизированная система управления инцидентами ИБ
- Автоматизированная система ведения БД знаний SOC
- Автоматизированная система ведения индикаторов компрометации
- Разработка автоматизированных процедур реагирования на инциденты ИБ (playbook)
- Разработка коннекторов и правил корреляции событий
- Автоматизированные средства проверки файлов на наличие вредоносного содержимого

Управление персоналом SOC

- Прием на работу специалистов SOC
- Организация сменной работы
- Обучение специалистов SOC
- Поддержание необходимой квалификации, проведение различного уровня тренингов
- Аттестация специалистов SOC
- Мотивация специалистов SOC
- Нормирование рабочей нагрузки каждой из линий SOC
- Формирование кадрового резерва

Пример структуры нормативной базы SOC

Политика мониторинга и реагирования на инциденты ИБ

Положение о SOC

Положение о ГРИИБ

- Регламенты по каждому их основных процессов SOC. Схемы процессов SOC с основными SLA
- Классификация инцидентов ИБ
- Инструкции по реагированию на основные типы инцидентов ИБ (описание сценариев - playbooks)
- Перечень прав доступа, необходимых для работы специалистов 1, 2, .. линии SOC
- Регламент управления источниками данных
- Правила аудита в информационных системах , системном ПО, специализированном оборудовании
- Инструкции для 1, 2 и .. линии SOC
- Инструкция по ведению базы индикаторов компрометации
- Положение по ведению базы знаний SOC
- Регламент сбора и обработки информации о новых угрозах (Threat Intelligence)
- Инструкция по обработки специализированных фидов (Финсерт, GroupIB, Bi.zone, PT и др.)
- Положение по обеспечению непрерывности работы SOC

Процессы

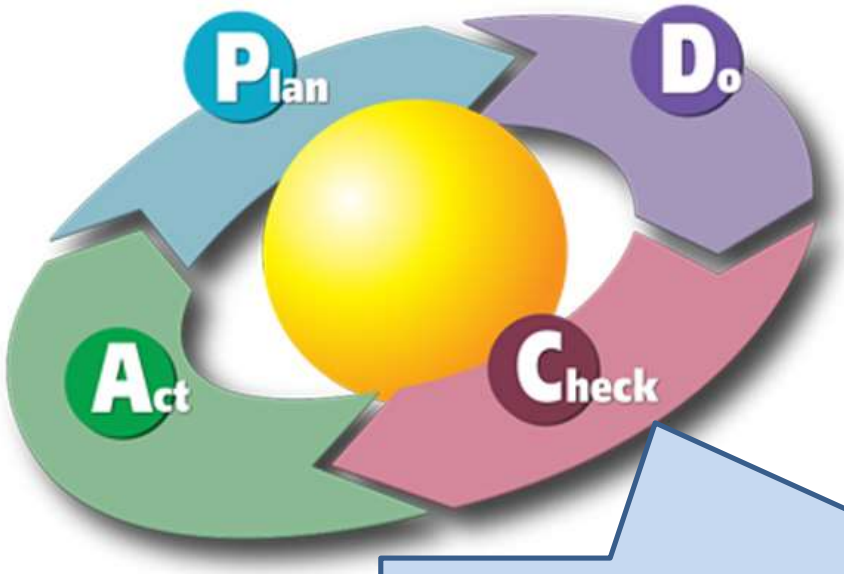
- Архитектура SOC
- Положения по администрированию средств и систем, обеспечивающих работу SOC
- Инструкции по настройке аудита на конкретных типах систем (могут входить в инструкции по настройке параметров ИБ для конкретных систем)
- Документация на правила анализа и корреляции собираемой информации
- Положение по разработки правил корреляции событий и поддержания их в актуальном состоянии

Технологии

- Программа поддержания уровня компетенций сотрудников SOC (обучение, ситуационные тренировки, штабные учения, тесты на проникновение, redteam, открытые киберучения)
- Квалификационные требования к сотрудникам сотрудников для каждой из линий SOC описанием тестов для приема на работу в SOC
- Параметры штатной нагрузки на каждую из линий SOC
- Положение по формированию кадрового резерва подразделения
- График сменной работы специалистов SOC
- Положение по аттестации специалистов SOC

Люди

Обеспечение ИБ – правильно выстроенные процессы



Внутренние и внешние аудиты SOC
Пентесты, в том числе в режиме RedTeam
Проверка выполнения SLA и ключевых метрик по каждому из основных процессов SOC
Анализ регулярных отчетов SOC

В части документов:
Положение по проведению киберучений
Регламент оценки эффективности работы SOC (с метриками эффективности в приложении)
Регламент отчетности SOC

Возможные метрики оценки эффективности SOC

	Метрика	Формула расчета
1	Процент ложноположительных Инцидентов ИБ	Отношение количества ложноположительных Инцидентов ИБ к общему количеству Инцидентов ИБ
2	Среднее время подтверждения подозрения на Инциденты ИБ	Отношение суммы времен подтверждения подозрения на Инцидент ИБ к общему количеству подтверждений
3	Среднее время регистрации Инцидентов ИБ IRP (перевод на 2 линию)	Отношение суммы времен регистрации Инцидентов ИБ IRP (перевод на 2 линию) к общему количеству регистраций
4	Среднее время информирования об Угрозе ИБ	Отношение суммы времен информирования об Угрозе ИБ к общему количеству информирований об Угрозах ИБ
5	Среднее время передачи нетиповых Инцидентов ИБ на 3 линию	Отношение суммы времен передачи нетиповых Инцидентов ИБ на 3 линию к общему количеству нетиповых Инцидентов ИБ
6	Среднее время выработки рекомендаций по реагированию на нетиповой Инцидент ИБ	Отношение суммы времени выработки рекомендаций по реагированию на нетиповой Инцидент ИБ к общему количеству нетиповых Инцидентов ИБ
7	Корректность мониторинга	Процент инцидентов без переклассификации в дальнейшем
8	Среднее время решения инцидента	Отношение суммы времен решения инцидентов за период к общему количеству инцидентов за период
9	Полнота покрытия сенсорами безопасности	Процент выявленных тестовых атак в разрезе активов (в отношении какого процента активов выявлена хоть одна атака)
10	Однородность мониторинга	Процент выявленных атак в зависимости от времени суток (разбивка по часам)
11	Уровень затрат на инцидент	Отношение затрат к подтверждённым инцидентам

Скородумов Анатолий Валентинович

E-Mail: Skorodumov@mail.ru

Телефон (812) 329-50-64

Благодарю за внимание!