БАНК САНКТ-ПЕТЕРБУРГ

Банк высокой культуры

Как оценить эффективность SOC конечному пользователю услуги?

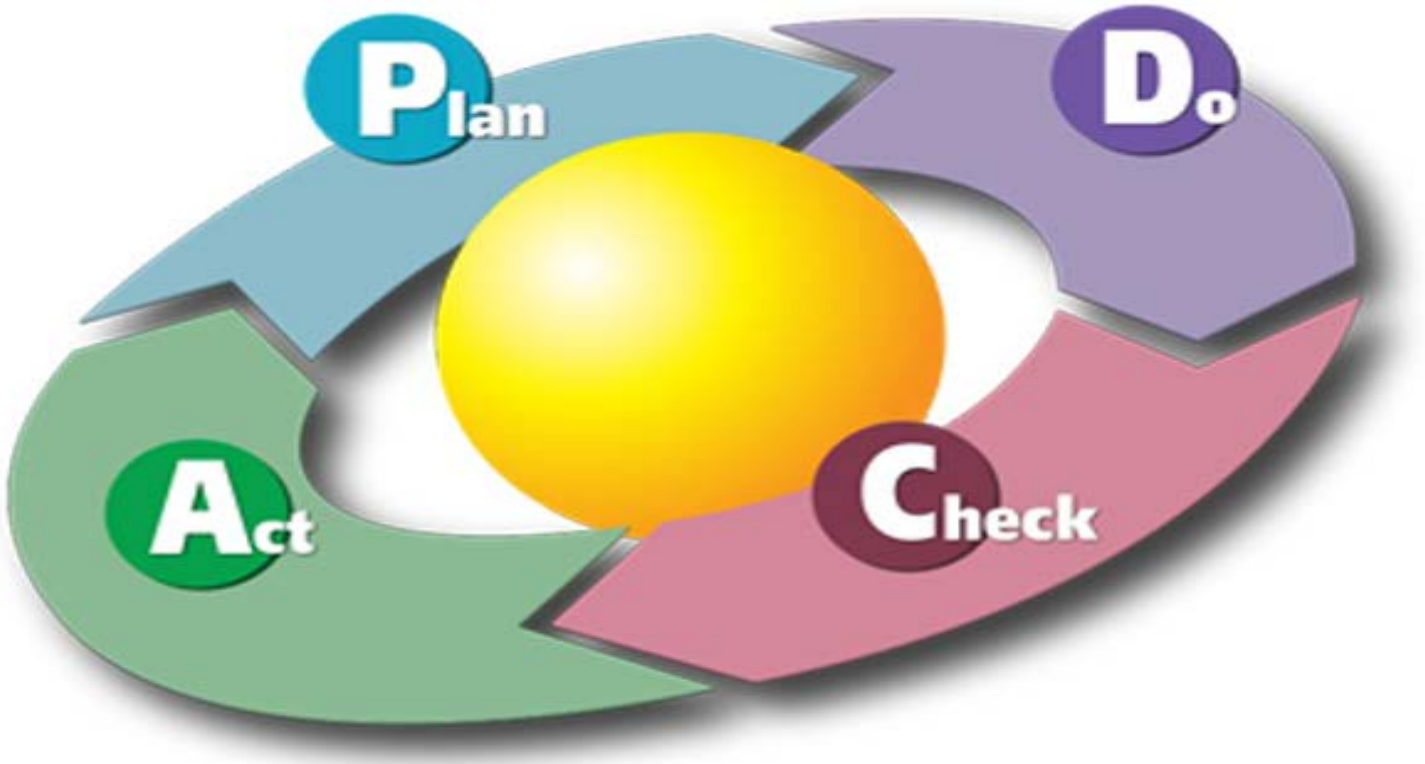
Скородумов Анатолий Валентинович

Заместитель директора –
Начальник управления по обеспечению информационной безопасности

Правильно прописанный SLA – основа для получения качественного сервиса

- Критерии качества сервиса
- Время обслуживания (получения сервиса)
- Порядок и сроки фиксации события (инцидента)
- Сроки реагирования
- Сроки решения проблемы
- Порядок эскалации решения проблемы
- Штрафные санкции

Обеспечение ИБ - это прежде всего правильно выстроенные процессы



SOC – это элемент процесса управления инцидентами ИБ. Оценка эффективности SOC – это элемент процесса контроля (Check).

Что оцениваем?

- Подается ли трафик со всех источников?
- Правильно ли разбираются поступающие логи?
- Какие правила настроены для обработки конкретных источников событий?
- Как настроены правила корреляции событий?
- Насколько глубоко осуществляется ручной анализ?
- Достаточно ли анализируемых в SOC событий для выявления реальных инцидентов?

Как оценить (работоспособность) эффективность SOC?

- Пентесты
- «Ложные» срабатывания
- Собственные проверочные тесты, индикаторы работоспособности правил

У вас произошел серьезный инцидент ИБ – кто виноват?

Чем характеризуется услуга SOC?

- Отсутствует реальная конкуренция на рынке услуг SOC
- Практически невозможно определить SLA
- Сложно оценить эффективность услуги
- Практически невозможно возложить ответственность за реальный инцидент на компанию, предоставляющую услугу SOC

Принцип получения качественной услуги SOC

Процесс управления инцидентами на базе SOC необходимо строить на принципах партнерства с компанией, предоставляющей услугу SOC

Принцип получения качественной услуги SOC

ДОВЕРЯЙ,

НО

ПРОВЕРЯЙ

БАНК
САНКТ-ПЕТЕРБУРГ

БАНК
САНКТ-ПЕТЕРБУРГ

Банк высокой культуры

Скородумов Анатолий Валентинович

E-Mail: Skorodumov@mail.ru

Телефон (812) 329-50-64

Благодарю за внимание!