Кибербезопасность 24x7 или жизнь SOC в непрерывном противодействии

Антон Юдаков
Операционный директор Центра мониторинга и реагирования на кибератаки Solar JSOC компании «Ростелеком-Солар»

Ростелеком
Солар

Solar JSOC #whoarewe

№1
на рынке SOC
в России

190+
сотрудников
Solar JSOC

72+ млрд
анализируемых
событий ИБ в сутки

10 минут
на обнаружение
кибератаки

30 минут
на реагирование
и защиту

50+
клиентов из топ-100
российского бизнеса

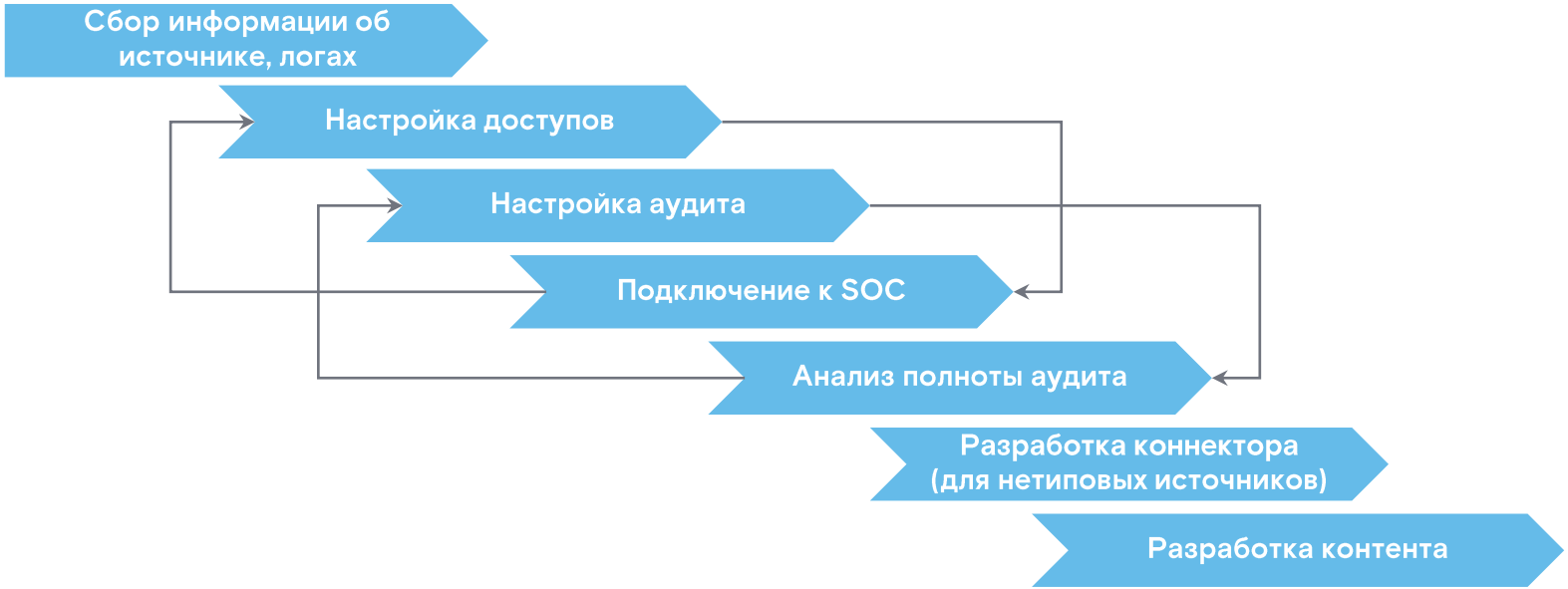
Ростелеком
Солар

Жизнь с клиентом – как в реальности?

Ростелеком
Солар

Источники событий – тернистый путь к результату

Для возможности мониторинга и выявления инцидентов ИБ нужно пройти тернистый путь:



Ростелеком
Солар

А потом путь еще тернистее

С чем мы сталкиваемся после:

- Проблемы с поступлением событий (истек пароль учетной записи, проблемы с сетевым доступом, источники мигрировали в другую подсеть, источник вывели из эксплуатации, подвисла сетевая шара и др.).
- Проблемы с аудитом (в результате перезаливки хостов, применения некорректных политик, пересмотра политик и др.).
- Проблемы с парсингом событий (обновили ПО на источнике, перешли на новую схему лицензирования и др.).
- И т.д.

Контент и сценарии мониторинга

Ведем ежедневный мониторинг и анализ актуальных угроз, методов их реализации и детекта:

- Информация по актуальным атакам, APT-кампаниям и угрозам с разбором malware (внутренние расследования, внешние источники)
- Информация о критичных уязвимостях
- Информация о новых методах проведения атак на разных стадиях
- Информация / исследование методов их детекта

Ростелеком
Солар

И даже в зрелой среде встречаются сюрпризы

А что у нас на периметре?

Кейс: достаточно зрелый заказчик, регулярные тестирования сервиса JSOC, сценариев, работают команды Red Team и Blue Team, проводятся регулярные внешние пентесты, но …

Успешный административный доступ из сети Интернет (7x.1xx.22x.8x|5432|192.168.1.10|5432|tcp)

База PostgreSQL, доступная из сети Интернет

Разбиение контента

Ростелеком
Солар

Жизнь с клиентом – а если проверить?

Ростелеком
Солар

Мы тестируем и нас тестируют

В ряде клиентов мы живем в режиме постоянного тестирования нашего сервиса, инфраструктуры заказчика и его команд реагирования

< 1 нед/мес

в среднем живём без тестирований

- **Внутреннее тестирование** сценариев перед запуском + регулярный анализ сработок нашими силами
- **Регулярное** тестирование контента
- **Пентесты**, проводимые у заказчиков
- Тестирование сервиса SOCa командой **Red Team Заказчика**

В случае пентестов и Red Team задача особенно актуальна тем, что тестирование производится произвольными методами, т.е. **не по нашим Playbook'ам.**

Тестирование – иногда больно, но оно того стоит

По результатам тестирований:

- Выявляются проблемы с полнотой аудита на конкретных хостах
- Выявляются неочевидные и сложно воспроизводимые самостоятельно ошибки корреляции
- Корректируется логика работы сценариев
- Появляются новые идеи для сценариев и сценарии мониторинга
- Выявляются узкие места в процессах реагирования
- Совместно с заказчиком планируются архитектурные и процессные изменения

Как охватить всю инфраструктуру?

Ростелеком
Солар

ИТ-инфраструктура – живой организм

- Изменение, оптимизация, развитие бизнес-процессов, ИТ-инфраструктуры
- Изменения в архитектуре систем и процессах работы с ними
- Внедрение новых информационных систем
- Слияние инфраструктур, централизация
- и т.д.

Ростелеком
Солар

Общий подход к мониторингу инфраструктуры:

Ключевая бизнес-инфраструктура

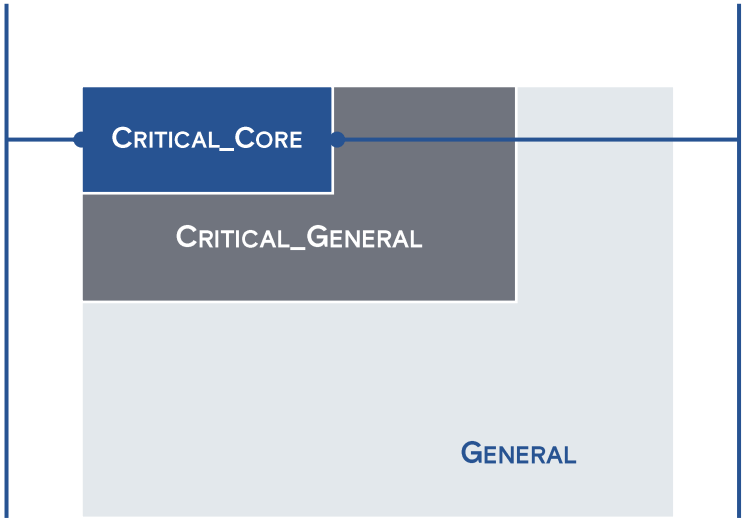
- Ключевая бизнес-инфраструктура (например, платежный сегмент и инфраструктура, ERP-система и др.)

Аудит событий:

- Расширенный аудит событий, использование EDR

Контроль состояния:

- Контроль поступления событий и полноты аудита
- Усиленный мониторинг доступности



Мониторинг инцидентов:

- Профилирование активности
- Максимальное покрытие сценариями мониторинга
- Часть сценариев являются специализированными для данного типа систем (прикладные)
- Регулярный Threat Hunting

Информирование:

- Повышенная критичность срабатываемых сценариев и дополнительная эскалация на заказчика

Тестирование:

- Регулярное тестирование всех сценариев мониторинга
- Регулярное тестирование командами Red Team и Blue Team

Общий подход к мониторингу инфраструктуры:

Критичная ИТ и ИБ инфраструктура

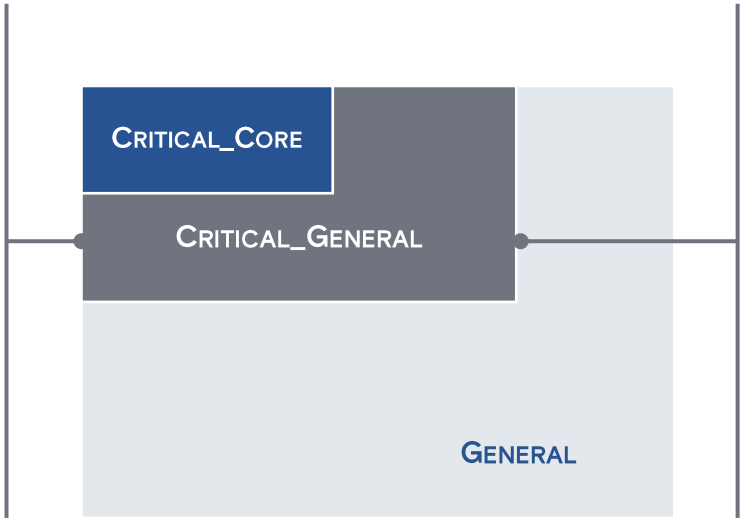
- Критичная ИТ и ИБ инфраструктура (например, DC, СЗИ, прокси, АРМ администраторов и т.д.)

Аудит событий:

- Расширенный аудит событий

Контроль состояния:

- Контроль поступления событий и полноты аудита
- Мониторинг доступности



Мониторинг инцидентов:

- Профилирование активности
- Максимальное покрытие сценариями мониторинга
- Регулярный Threat Hunting

Информирование:

- Дополнительная эскалация на заказчика при подозрительной активности

Тестирование:

- Регулярное тестирование выборочных сценариев мониторинга

Общий подход к мониторингу инфраструктуры:

Остальная не критичная инфраструктура

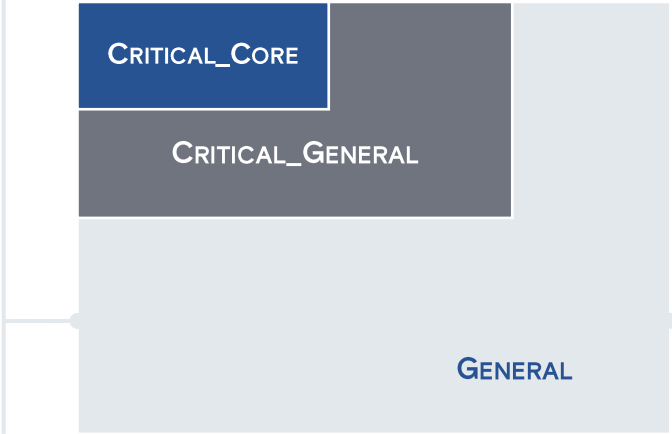
- Общая инфраструктура (например, обезличенная тестовая среда, АРМ обычных пользователей и т.п.)

Аудит событий:

- Общий рекомендуемый аудит событий

Контроль состояния:

- Сбор и мониторинг событий могут не осуществляться, но источник доступен для подключения при необходимости
- Косвенный мониторинг осуществляется посредством критичных инфраструктурных систем (АВПО, SCCM, DC, proxy, FW и т.п.)



Мониторинг инцидентов:

- Общие инфраструктурные сценарии мониторинга, работающие на скоупе Critical_General

Информирование:

- Дополнительная эскалация на заказчика при массовых сработках или отдельных критичных событиях

Тестирование:

- Регулярное тестирование выборочных сценариев мониторинга

Подводя итог

Ростелеком
Солар

Жизнь с клиентом – как в реальности

Для повышения эффективности внешнего сервиса SOC максимально важны постоянная коммуникация и взаимодействие с заказчиком – operations-жизнь с клиентом, а также постоянная проверка и совершенствование

При этом:

- Распределяем усилия
- Совместно развиваем архитектуру ИБ и покрытие мониторингом
- Разделяем, но синхронизируем активности

- **Пример:** выделение группы критичных серверов в отдельную подсеть, организация доступа к ним через выделенный терминальный сервер, организация соответствующего мониторинга

  Как результат: повышение контролируемости активности, возможность выявления аномалий, нарушения политик доступа

Спасибо за внимание!

Антон Юдаков
Операционный директор Центра мониторинга и реагирования на кибератаки Solar JSOC компании «Ростелеком-Солар»

Ростелеком
Солар