

Ampire 360°



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Ampire 360°

ПОЛИГОН КИБЕРБЕЗОПАСНОСТИ



Threat Intelligence

SOC & DFIR

Offensive Security

Киберучения

ИИ и киберзащита

Киберполигон Ampire

📅 14 октября





Почему СЗИ не работают

Правда эксплуатации

Соседова Надежда

старший инженер по информационной
безопасности

Перспективный мониторинг



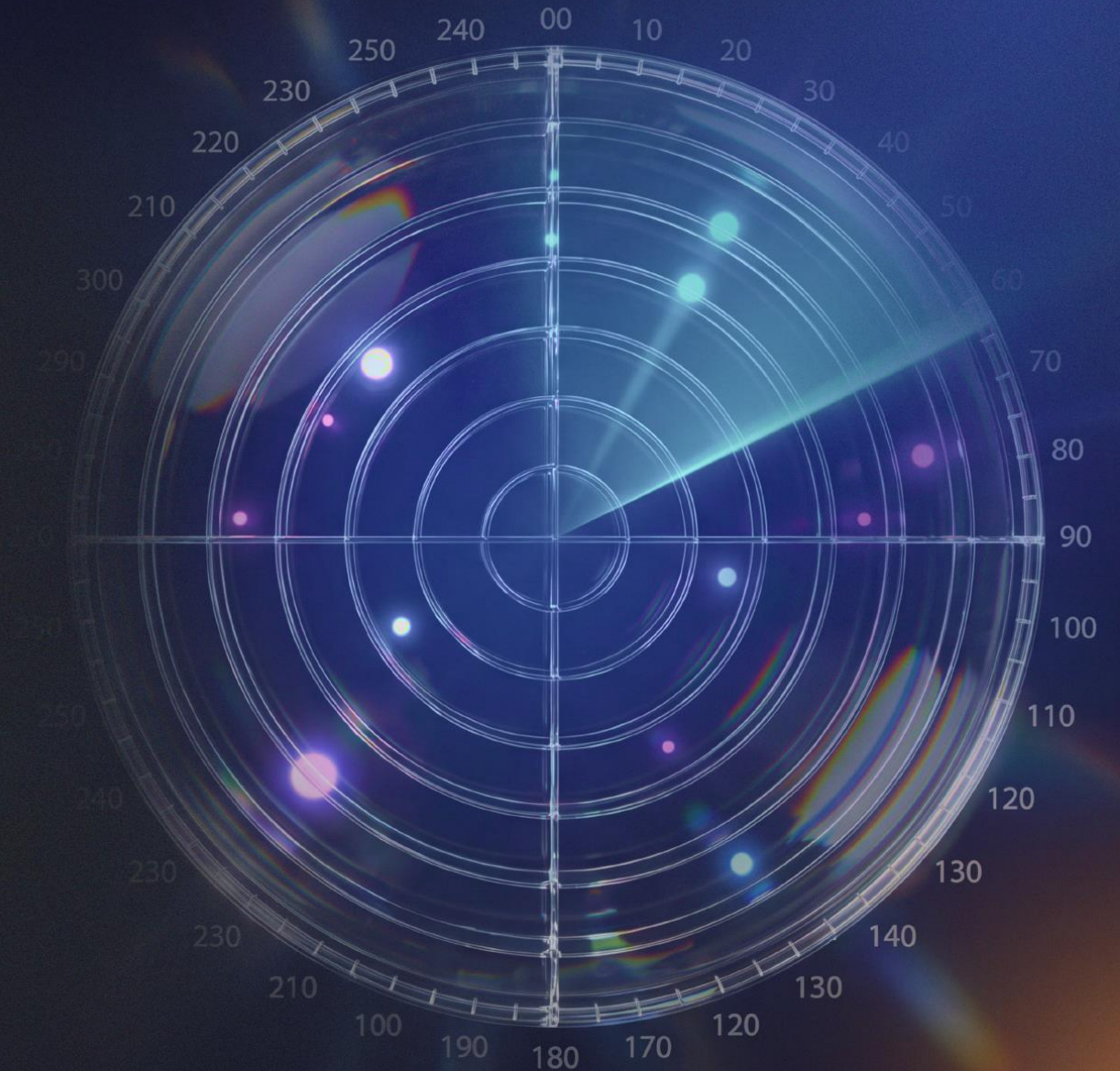
ООО «Ромашка»

Ampire 360°

- СЗИ установлены (Firewall, EDR, IDS/IPS, Антивирус, SIEM и т.д.)
- Настроены политики безопасности
- Вся инфраструктура покрыта СЗИ
- У администраторов десятки консолей с зелеными статусами агентов
- У руководства красивые отчеты каждую неделю

Происходит атака и часть действий злоумышленника остается незамеченной

Почему СЗИ не отработали?



СЗИ может «не работать» еще до начала эксплуатации



Важно: установить – не значит внедрить

Включить все правила ≠ обеспечить обнаружение атак

СОВ не знает контекста

- Не понимает, какая сеть внешняя, а какая защищаемая
- Не знает, какие сервисы реально работают
- Не учитывает на каких портах и по каким протоколам работают сервисы в конкретной организации
- Генерирует множество ложных срабатываний на нормальный трафик
- Может неверно интерпретировать трафик
- Часть атак проходит незамеченной

СОВ знает контекст

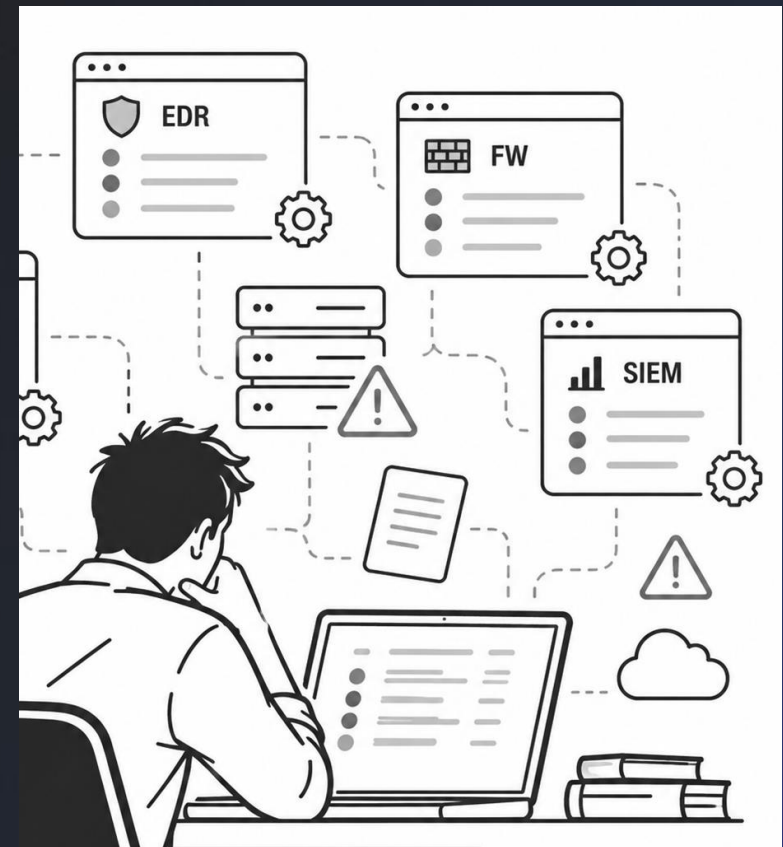
- Понимает границы защищаемой инфраструктуры
- Учитывает функционирующие сервисы
- Учитывает используемые сервисами порты и протоколы
- Точнее применяет сигнатуры
- Уменьшается число ложных срабатываний
- Дает более полезные и приоритетные события для анализа

Настройка СЗИ – сложная инженерная работа

Качественная настройка СЗИ не является только выполнением последовательности шагов, для ее успеха требуется комплекс инструментов

Документация – отвечает на вопросы: «Где настройка?», «Какие у меня есть варианты?»

Бэкграунд инженера – позволяет принять решение о необходимости настройки в инфраструктуре, опираясь на понимание работы сетей/ОС/приложений/способов реализации атак



Важно: Документация на СЗИ не знает вашу инфраструктуру

Защита охраняет «вчерашнюю» инфраструктуру



Важно: изменилась инфраструктура – должна измениться модель защиты

Как не дать защитной модели устареть

Встроить ИБ в change management

Каждое изменение сервиса, сети или доступа должно иметь ответ на вопрос: Что меняется в модели защиты?

Делать ревью правил

Регулярно проверять МЭ, COB, EDR и т.д. на предмет устаревших исключений, избыточных правил и доступов без владельцев

Ограничивать временные доступы

Каждое исключение должно иметь владельца, срок жизни и понятную причину

Связывать ИТ и ИБ

Новый актив или сегмент должен автоматически попадать в контур контроля

Защиту нельзя просто выкрутить на максимум

Мягкая политика

Последствия: меньше конфликтов с процессами, но больше возможностей для злоумышленника

Жесткая политика

Последствия: меньше риска пропуска атаки, но выше риск остановить нормальную работу

Разумный баланс
Управляемый риск

Важно: Больше блокировок ≠ больше защиты

Одна цепочка – разные смыслы



Защита теряет эффективность постепенно

Ampire 360°



Ничего не было выключено, а защитных функций стало меньше

Средства защиты видят атаку по частям

Что происходит	Как события могут выглядеть без общего контекста
Пользователь получает фишинговое письмо	Входящее электронное письмо
Учетные данные пользователя используются для входа в систему	Событие успешного входа под известным пользователем
Злоумышленник запускает PowerShell и обращается к соседнему серверу	Запуск процесса
Злоумышленник собирает информацию с сервера в архив	Использование приложения для архивирования
Передает архив с информацией на сторонний сервер	Исходящий трафик по стандартному порту

Важно: необходимо проводить корреляцию событий с разных СЗИ

Пентест: Сетевая атака -> Подбор пароля -> Подключение по SSH

Учетные данные

Пароли по умолчанию
облегчили перебор пароля

Антивирус

Журналирование выключено
Сетевые атаки не зафиксированы

IDS

События отправлялись в SIEM,
но правила давно не обновлялись

SIEM

Неполное покрытие сценария

Проверяем функцию, а не статус

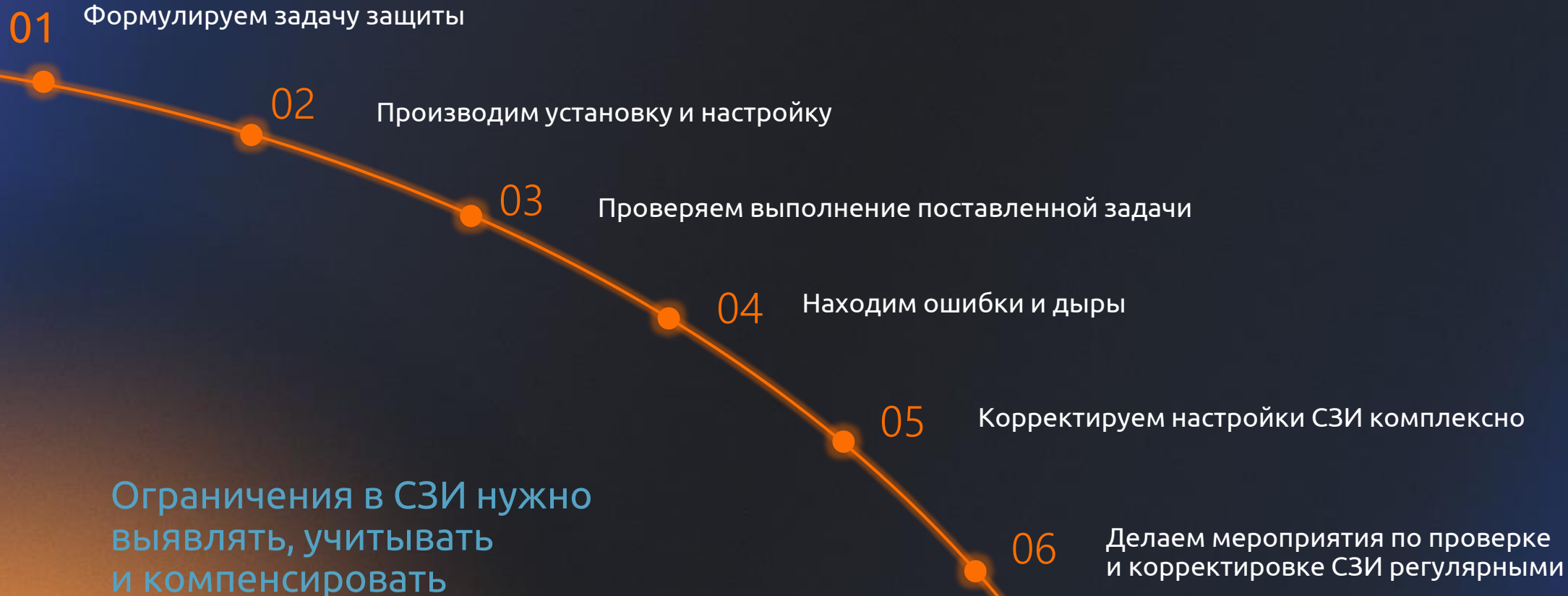
«Зеленый» статус

- Агент СЗИ онлайн
- Службы СЗИ запущены
- Базы/ сигнатуры обновлены
- Лицензия активна
- Политика назначена
- События с агента поступают в консоль управления
- В событиях информации об ошибках и авариях нет

Защитная функция

- Генерируем контролируемое тестовое событие
- Проверяем, что событие попало в нужную зону контроля
- Убеждаемся, что СЗИ корректно его распознало
- Проверяем, что сработало нужное правило или политика
- Проверяем, что сработала предусмотренная цепочка реагирования

У всех СЗИ есть нюансы, главное – добиться результата



Благодарю за внимание

Соседова Надежда

старший инженер по информационной безопасности

Перспективный мониторинг



Ampire 360°