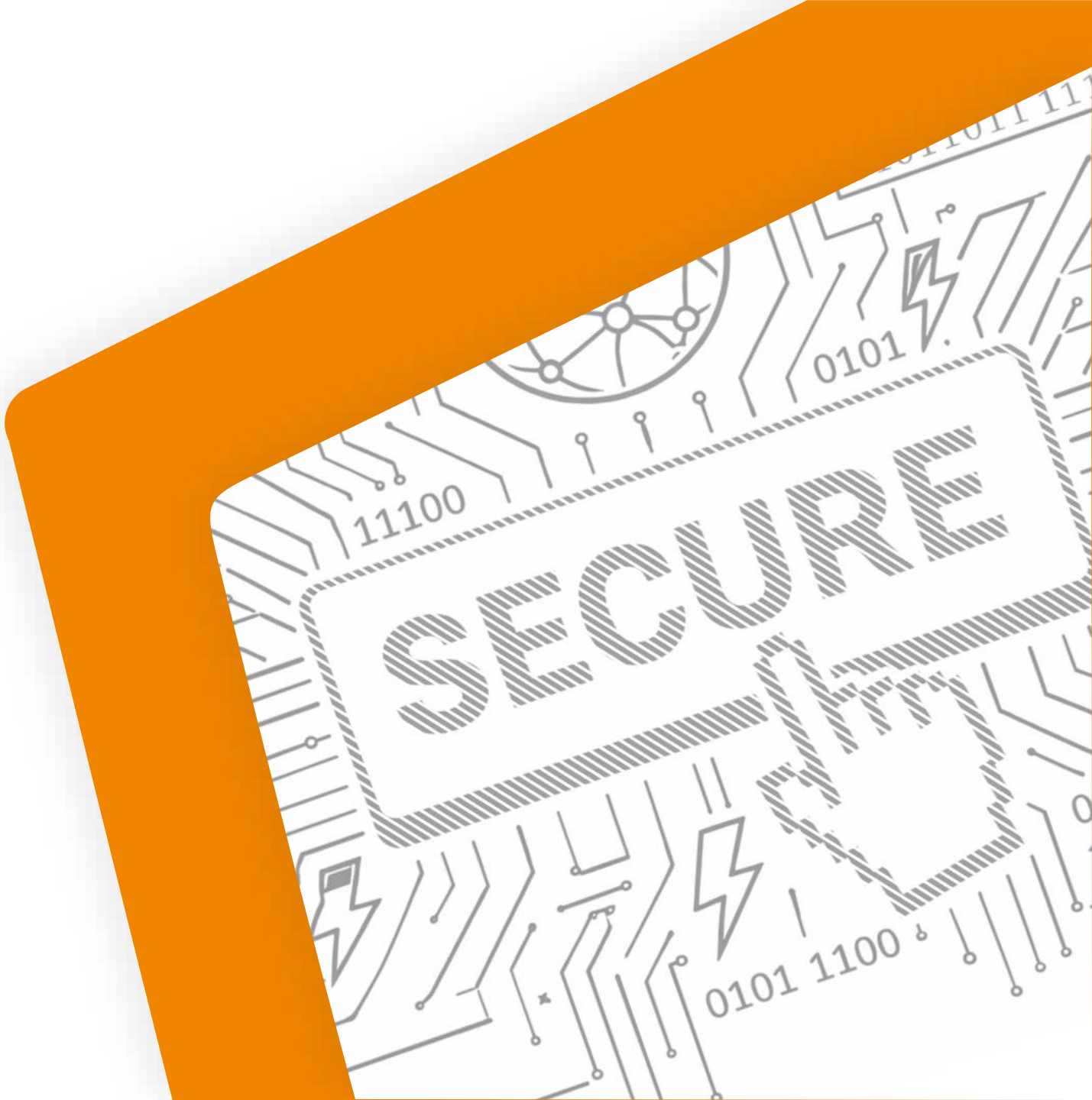
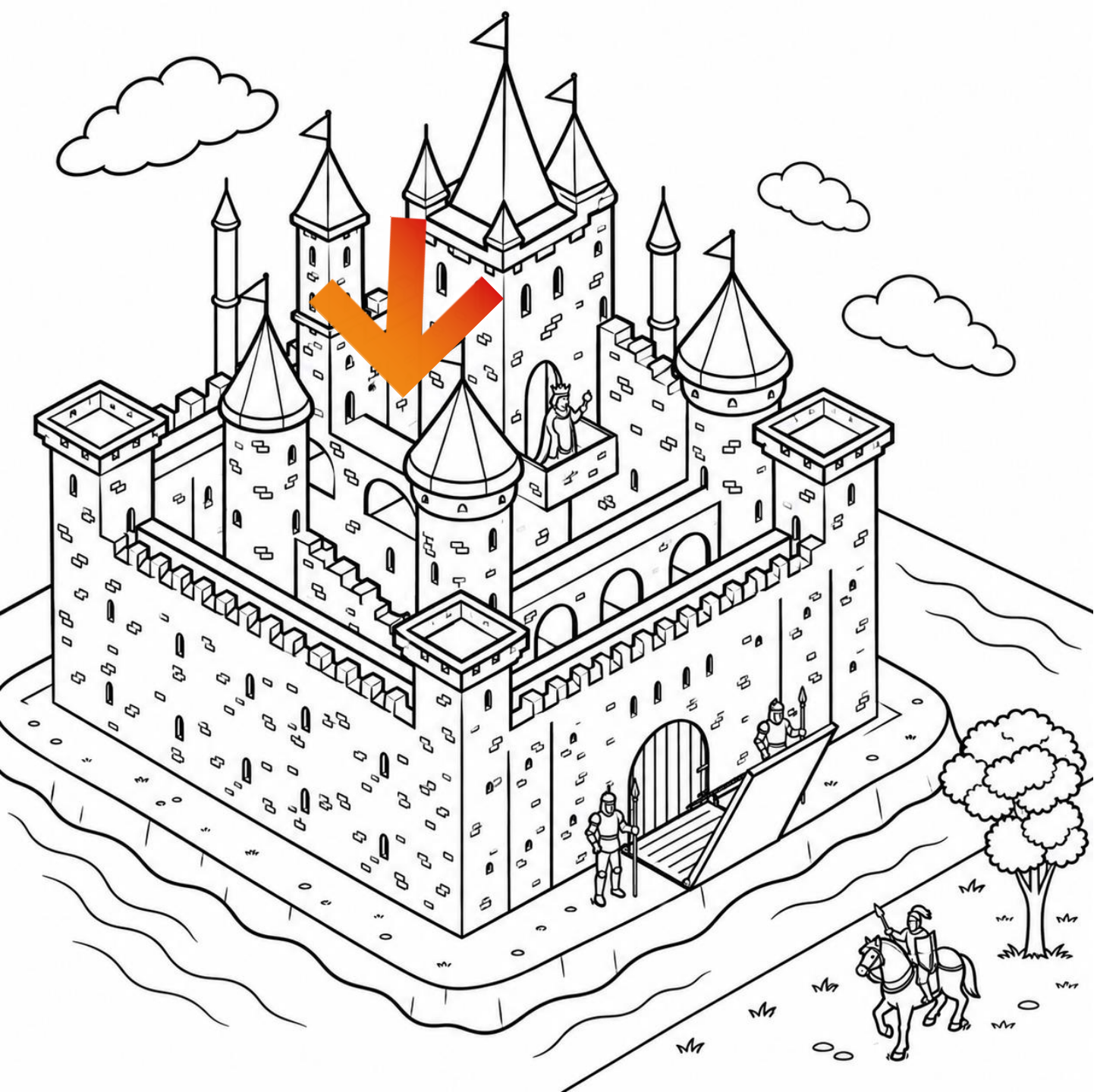
ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Охота на призраков: как понять, что инфраструктура не скомпрометирована

Софья Карева,
менеджер продукта

Денис Ермаченко,
начальник отдела расследования
компьютерных инцидентов





Zero Trust

Злоумышленник уже внутри сети

А вы уверены, что прямо сейчас в вашей инфраструктуре нет злоумышленника?

- Как это определить?

Compromise Assessment ≠ пентест

Решение	Вопрос
Пентест	«Можем ли мы взломать этот процесс?»
Анализ защищенности	«Какие уязвимости и слабые места у нас есть?»
Red Team	«Смогут ли атакующие пробиться, противодействуя защите?»
SOC	«Что происходит в инфраструктуре прямо сейчас?»
Compromise Assessment	Есть ли признаки того, что инфраструктура уже скомпрометирована или была скомпрометирована?»

Фокус на поиске фактов и артефактов уже состоявшейся или продолжающейся компрометации

Compromise Assessment

Выявление следов компрометации

Углубленная проверка ИТ-инфраструктуры Заказчика для выявления признаков скрытого или ранее незамеченного компрометационного воздействия, а также оценки устойчивости организации к киберугрозам.

- Своевременное обнаружение киберугроз
- Минимизация последствий возможных инцидентов ИБ
- Полноценная проактивная защита инфраструктуры
- Минимизация проведения повторной атаки
- Снижение рисков компрометации

Когда стоит делать Compromise Assessment?

После серьёзного инцидента

Даже если инцидент локализован, злоумышленник может оставаться в инфраструктуре или иметь доступ к данным

Слияния и поглощения

Объединение организаций, подключение региональных подразделений к общей инфраструктуре

Изменение ИТ-ландшафта

Трансформация инфраструктуры, объединение доменов, миграция в облако, внедрение новых систем

Уязвимость на периметре

Эксплуатация часто начинается раньше патча: обновление закрывает дверь, но не показывает, кто уже вошёл

Косвенные признаки

Утечка, о которой узнали извне, неизвестные учётные записи, письма, которых вы не отправляли

Регулярная независимая проверка

Даже при наличии SOC полезно периодически проверять инфраструктуру. Рекомендуем регулярно, например раз в квартал

Compromise Assessment

Пошаговая логика проверки:
от triage до технического заключения

0 Старт

Подключение к инфраструктуре Заказчика, согласование гипотез и перечня систем для проверки

Результат: подтверждены контур проверки, критичные узлы и необходимые доступы

1 Сбор артефактов

- Получение triage с рабочих станций и серверов
- Выгрузка журналов, EDR/SIEM и сетевых событий
- Приоритизация критичных систем

2 Проверка узлов

- Анализ процессов, сервисов, задач и автозапуска
- IOC- и YARA-hunting
- Проверка подозрительной сетевой активности

3 Анализ AD

- Проверка привилегий, входов, GPO и сервисных учётных записей
- Поиск горизонтальных перемещений и механизмов закрепления

4 Подтверждение

- Корреляция найденных артефактов и индикаторов
- Анализ вредоносных объектов при обнаружении
- Определение затронутых узлов

5 Отчёт

- Техническое заключение о наличии или отсутствии признаков компрометации
- Перечень рисков и рекомендации по снижению

Что получает Заказчик: объективную картину состояния инфраструктуры, подтверждённые находки и рекомендации по дальнейшим действиям

Какие данные мы собираем?

Источник	Что ищем
Серверы и рабочие станции	Следы запусков, журналы событий, механизмы закрепления, оперативная память
Домен и учётные записи	Новые привилегированные записи, изменения политик, признаки выгрузки хэшей
Сеть	Связь с серверами атакующего, нетипичный исходящий трафик, внутренние подключения
Периметр и почта	Входы из необычных мест и времени, следы эксплуатации, правила пересылки
Облако и SaaS	Выданные приложениям права, новые правила, подозрительные входы

Администратор или злоумышленник?

Кто?

Роль учётной записи подходит к действию?

Откуда?

Административная станция или рабочее место сотрудника?

Когда?

Окно работ или три часа ночи в выходной?

Чем?

Инструмент из вашего стандарта или чужой?

Зачем?

Есть заявка на изменение и подтверждение владельца?

Решает контекст, а не инструмент!

Дополнительно смотрим на последовательность действий, их редкость, сокрытие следов и отклонение от нормы.

«Вот инфраструктура – разберись сам» – не сработает!

Заказчик помогает:

- Понять инфраструктуру
- Определить критические системы
- Объяснить особенности инфраструктуры
- Предоставить необходимо данные
- Оперативно уточнять обнаруженные события

Исполнитель делает:

- Формирует гипотезы поиска
- Проводит технический анализ
- Сопоставляет артефакты
- Ищет признаки компрометации
- Формирует выводы и рекомендации

Чем лучше взаимодействие команд, тем полнее итоговая картина!!!

Мифы о Compromise Assessment

CA сводится к антивирусной проверке

Анализируем следы действий: запуски, входы, закрепление, сетевые связи, а не только файлы

Если ничего не нашли, взлома не было

Это отсутствие признаков в рамках охвата, периода и доступных данных

Удалили файл и сменили пароль, инцидент закрыт

Пока не найдены вектор и все механизмы закрепления, у атакующего остаются запасные входы

SOC и SIEM делают CA ненужной

SOC видит только подключённые источники; проверка даёт независимый взгляд и показывает слепые зоны

Даёт тот же результат, что пентест

Пентест ищет пути проникновения, проверка ищет следы реального присутствия атакующего



Как честно читать результат?

Ограничения метода:

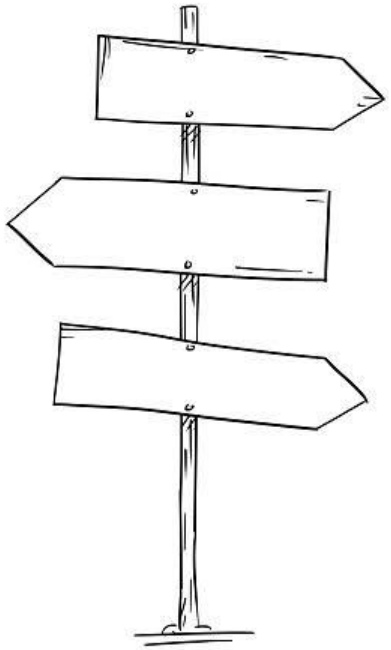
- Срез во времени
- Доступность данных и журналов
- Границы охвата
- Шифрованный трафик



Проверка показывает отсутствие признаков компрометации при заданном охвате, но не доказывает её отсутствие

Как честно читать результат?

Компрометация обнаружена	Переходим к реагированию
Есть подозрения, вывод неоднозначен	Нужны уточнения и данные
Признаков не найдено	Вместе с охватом, периодом и слепыми зонами



Что должно быть в хорошем отчете?

Самая ценная часть проверки – это не вердикт, а побочный результат

- Границы и период проверки
- Перечень источников и их полноту
- Методика проверки
- Находки с описанием степени уверенности
- Слепые зоны инфраструктуры с рекомендациями по закрытию
- Рекомендации для технической и бизнесовой команды

Если все чисто – относимся с осторожностью

Спецпредложение

Первичный поиск признаков компрометации

- До 5 узлов одного согласованного участка инфраструктуры
- Один цикл сбора и анализа
- Первичная проверка выявленных подозрительных объектов и событий

Результат: краткое экспертное заключение с находками и рекомендациями



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо за внимание!

amonitoring.ru

Наши контакты

+7 (495) 737-61-97
info@amonitoring.ru