ГАЙД ДЛЯ НАЧИНАЮЩИХ • 20 СЛАЙДОВ

ГЛУБОКАЯ ЗАЩИТА

Ваш firewall не спасёт.

Это не ошибка в настройке, а целостный подход к безопасности. Нельзя полагаться только на один слой — нужна полноценная многоуровневая защита.



ВНЕШНИЕ СЛОИ ПРОБИТЫ

ТРЕТИЙ СЛОЙ УДЕРЖАЛ

Листайте, чтобы увидеть все семь слоёв →

@lionsoulbatyshchikov

ГЛАВНАЯ ПРОБЛЕМА • 02/20

ОДНА СТЕНА, ОДНО ПАДЕНИЕ

Большинство систем строятся по одному и тому же принципу: жёсткий контроль на границе и «мягкое» доверие внутри.



Доверие внутри

За пределами границы все устройства часто считаются доверенными по умолчанию.

Нет видимости

Система фиксирует только то, что было заблокировано, а не то, что прошло внутрь.

Нет второй линии

После прохода через границу нет дополнительных проверок, поэтому атака не замедляется.

НАСТОЯЩАЯ ПРОБЛЕМА

Контроль, которому вы полностью доверяете, — это не стена, а **единая точка отказа** (single point of failure).

ПОЧЕМУ СУЩЕСТВУЮТ СЛОИ • 03/20

КАЖДЫЙ КОНТРОЛЬ В РЕАЛЬНОСТИ РАНО ИЛИ ПОЗДНО ДАЁТ СБОЙ

Не если, а когда. Существует только четыре основных причины и ни одна из них не является редкой.

01

ОБХОД (BYPASSED)

Атакующий находит способ обойти контроль. Например, жёсткий корпоративный ноутбук оказывается заражён через домашнюю сеть.

02

НЕПРАВИЛЬНАЯ НАСТРОЙКА (MISCONFIGURED)

Контроль включён, но настроен неправильно. Например, правило создали для теста, общая папка осталась публичной, а дефолтная конфигурация так и не была изменена.



03

НЕИЗВЕСТНАЯ УЯЗВИМОСТЬ (UNKNOWN)

Уязвимость без известного решения. В день появления нового бага даже полностью обновлённая система остаётся уязвимой.



04

ЧЕЛОВЕЧЕСКИЙ ФАКТОР (HUMAN)

Кто-то помог не тому. Убедительный звонок, спешка, случайный клик или симпатия к новому коллеге — и контроль срабатывает против вас.



ГЛАВНЫЙ ВЫВОД

Контроль — это не гарантия, а только **вероятность**.
Глубокая защита достигается за счёт того, что множество небольших вероятностей перемножаются в очень маленькую.

@lionsoulbatyshchikov

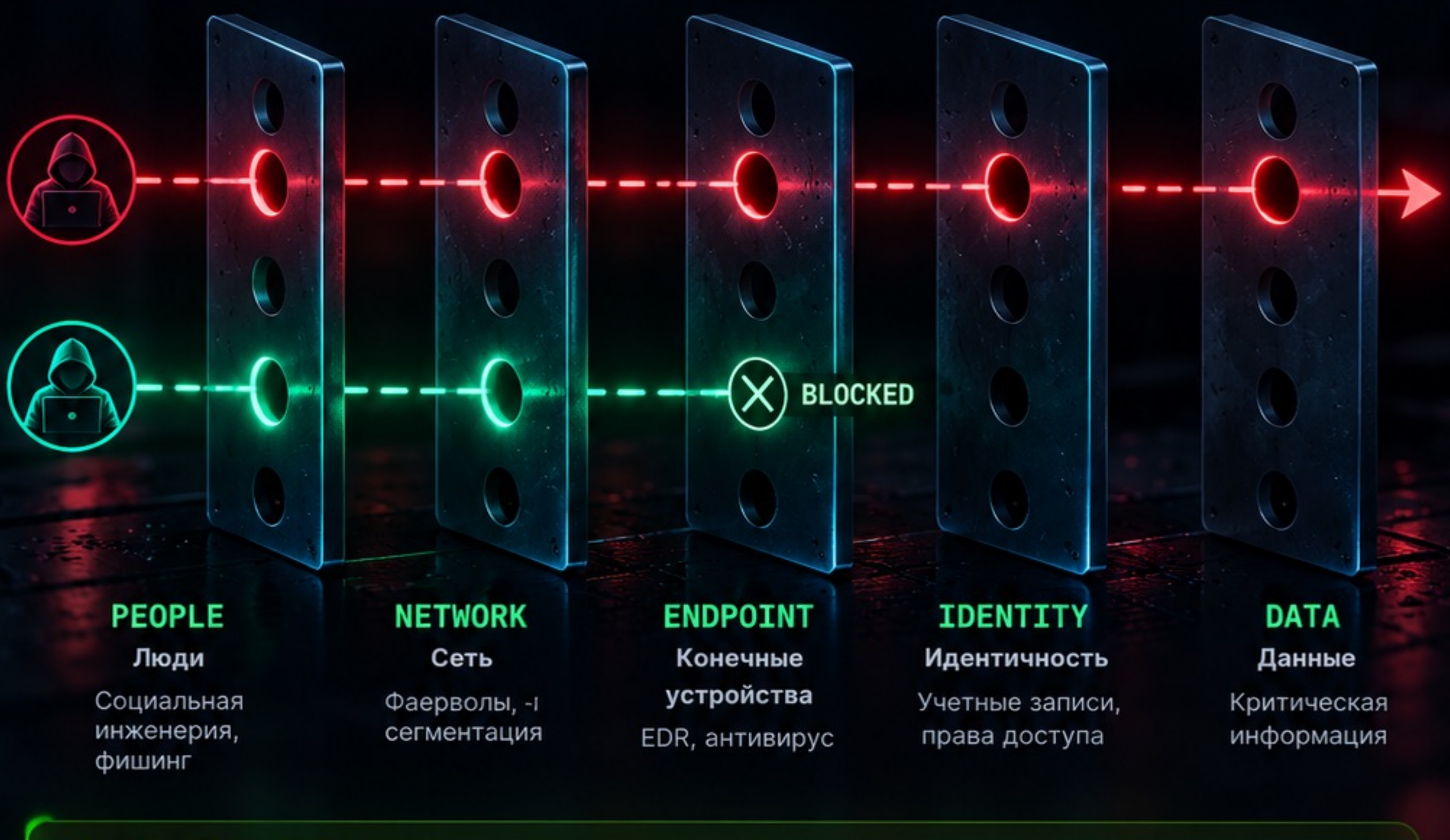
МОДЕЛЬ АТАКИ • 04/20

КОГДА ОТВЕРСТИЯ СОВПАДАЮТ

Каждый слой защиты имеет свои «отверстия»: то, что он не видит, не может достичь или не был предназначен перехватить.
Один инцидент — это не просто сбой, а совпадение отверстий по всей цепочке.

ПОПЫТКА 1
Заблокирована

ПОПЫТКА 2
Все пять отверстий совпали



PEOPLE
Люди
Социальная инженерия, фишинг

NETWORK
Сеть
Фаерволы, -ı сегментация

ENDPOINT
Конечные устройства
EDR, антивирус

IDENTITY
Идентичность
Учетные записи, права доступа

DATA
Данные
Критическая информация

ГЛАВНЫЙ ВЫВОД

Один и тот же атакующий, две попытки.
Вторая сработала только потому, что пять отдельных пробелов совпали и оказались **на одной линии.**

@lionsoulbatyshchikov

ОПРЕДЕЛЕНИЕ • 05/20

ЧТО ЭТО ТАКОЕ НА САМОМ ДЕЛЕ?

Несколько независимых контролей, выстроенных так, чтобы ни один единичный сбой не дал атакующему достичь своей цели.

01 ИЗНАЧАЛЬНО ПЛАНИРУЙТЕ С УЧЁТОМ СБОЕВ

Проектируйте каждый слой так, как будто предыдущий уже скомпрометирован. Одна точка отказа не должна разрушать всю защиту.



02 ИСПОЛЬЗУЙТЕ РАЗНЫЕ ТИПЫ КОНТРОЛЕЙ

Второй контроль, который ломается так же, как и первый, — это не защита. Варьируйте типы: технические, процессные, организационные, детективные и превентивные. Важно разнообразие, а не просто количество.



03 УЧИТЫВАЙТЕ ВРЕМЯ И ШУМ

Каждый дополнительный слой отнимает у атакующего время и увеличивает шанс ошибки. Время — это то, на чём держится ваше обнаружение (detection).



ГЛАВНЫЙ ВЫВОД

Defense in Depth — это не готовый продукт, который можно купить. Это **архитектура, которую вы проектируете**.

@lionsoulbatyshchikov

КАРТА ЗАЩИТЫ • 06/20

СЕМЬ СЛОЁВ ЗАЩИТЫ

Снаружи внутрь. Каждый слой решает свою задачу, поэтому одна и та же техника атаки редко срабатывает дважды. Атакующему приходится пройти через все слои.



07 PEOPLE & POLICY
Люди и процессы
Права, обучение, процедуры, политика.

06 PHYSICAL
Физическая безопасность
Доступ в помещения, серверные, стойки.

05 NETWORK
Сеть
Сегментация, межсетевые экраны, нарушение связности.

04 ENDPOINT
Конечные устройства
Рабочие станции, серверы, EDR/AV.

03 IDENTITY
Идентичность
Учетные записи, аутентификация, права доступа.

02 APPLICATION
Приложения
Бизнес-логика, уязвимости в коде, конфигурации.

01 DATA
Данные
То, ради чего всё это происходит.

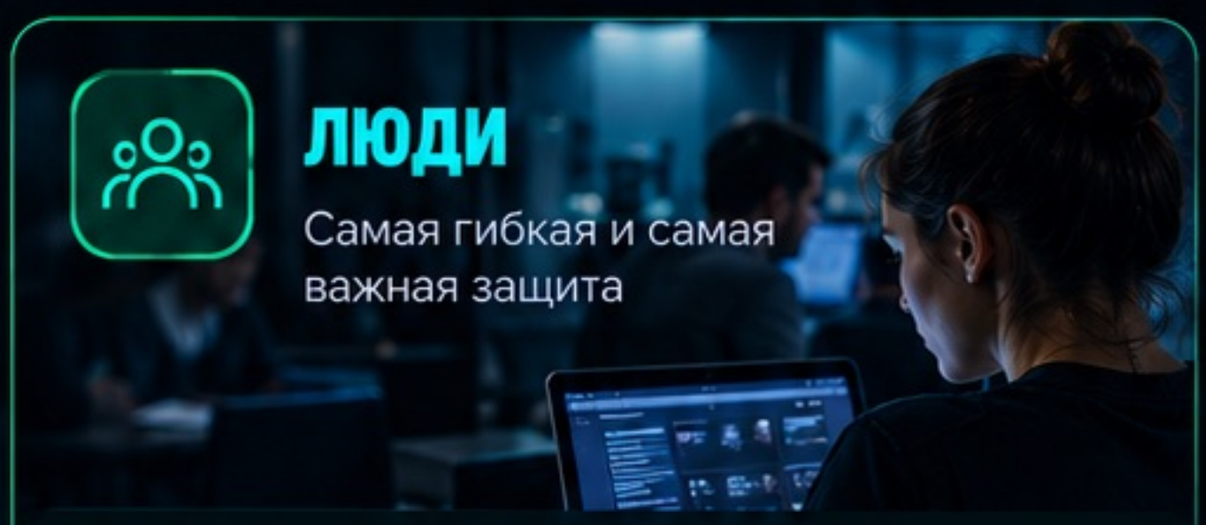
ВАЖНО

Это практическая модель, а не жёсткий стандарт.
Названия могут отличаться — **суть остаётся той же.**

СЛОЙ 07 + 06 • 07/20

ЛЮДИ И ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

Эти два слоя часто недооценивают. Никакой софт не поможет, если в здание зайдёт посторонний или убедительное сообщение заставит сотрудника выдать доступ.



ЛЮДИ

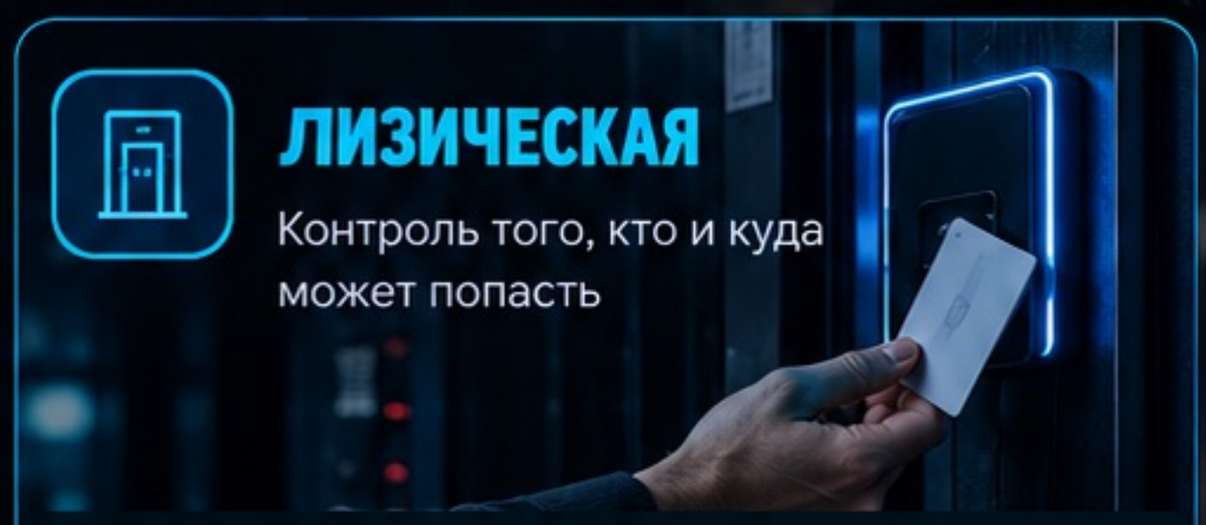
Самая гибкая и самая важная защита

Простая система сообщений
Один клик для сообщения об инциденте работает быстрее любых фильтров.

Короткое и регулярное обучение
Частые и короткие сессии эффективнее длинных презентаций раз в год.

Культура без обвинений
Люди спокойно сообщают о своих ошибках.

Изменение ролей
Приход, перевод, уход — доступы следуют за ролью, а не за конкретным человеком.



ЛИЗИЧЕСКАЯ

Контроль того, кто и куда может попасть

Бейдж на каждой двери
Один бейдж — один человек.
Нет «просто зайду».

Сопровождение гостей
Посетители всегда с сопровождающим, включая подрядчиков.

Закрытые стойки и серверные
Физический доступ ограничен.
Кабели — это тоже поверхность атаки.

Безопасная утилизация устройств
Носители очищаются перед списанием.
Старые диски всё ещё «разговаривают».

ПРЕДОТВРАЩАЕТ

- ✓ Несанкционированный доступ в здание
- ✓ Проход по чужому бейджу (tailgating)
- ✓ Потерю рабочих устройств
- ✓ Утечку данных через человеческий фактор

ВСЁ ЕЩЁ ПРОПУСКАЕТ

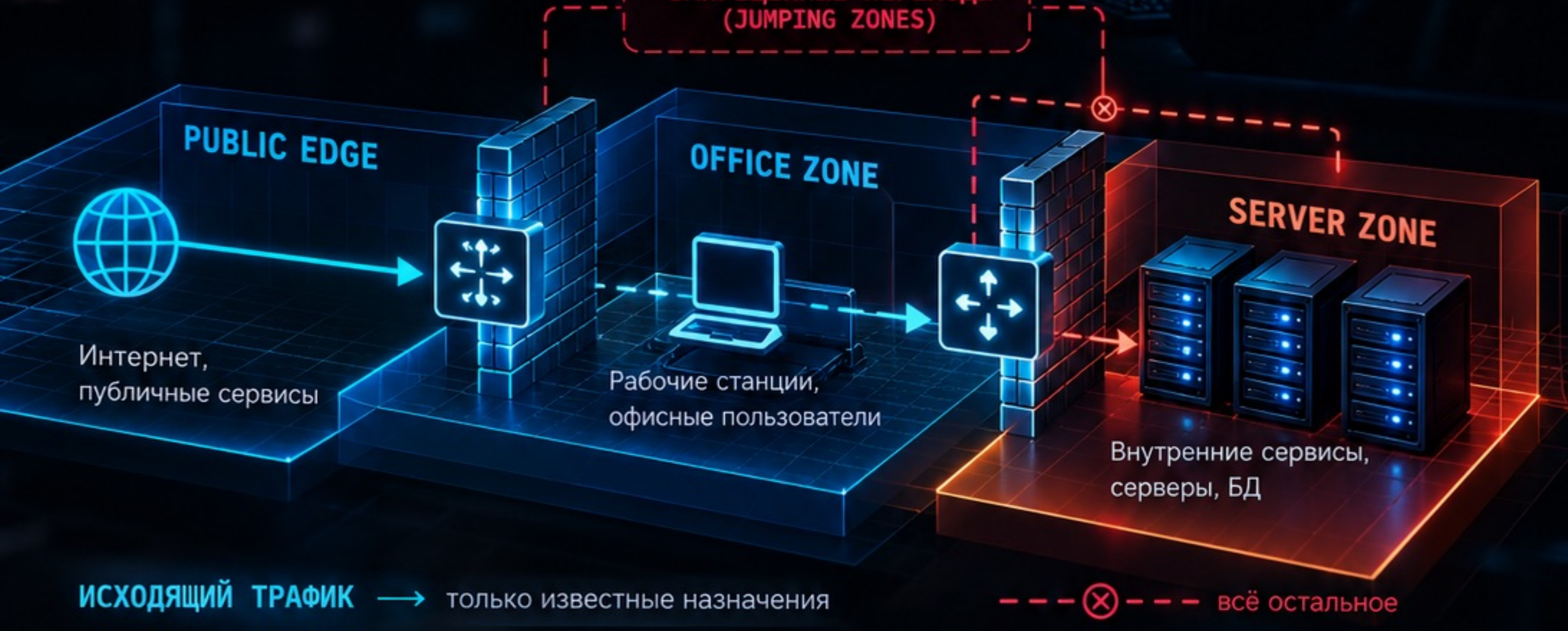
Хорошо подготовленный звонок от **«коллеги»** всё ещё может заставить человека выдать доступ.



СЛОЙ 05 • 08/20

ПЕРИМЕТР И СЕТЬ

Это дороги между системами. Этот слой решает, кто с кем может общаться, в каком направлении и что разрешено покидать инфраструктуру.



КОНТРОЛИ В ЭТОМ СЛОЕ

Deny by default
Запрещено по умолчанию

Segmented zones
Сегментация сети

Traffic monitoring
Мониторинг трафика

Egress filtering
Фильтрация исходящего трафика

Encrypted access
Шифрование соединений

ПРЕДОТВРАЩАЕТ

Ненужное сканирование извне и неконтролируемое перемещение между сегментами.

ПРОПУСКАЕТ

Обычный зашифрованный трафик к популярным сервисам (например, обновления, SaaS).

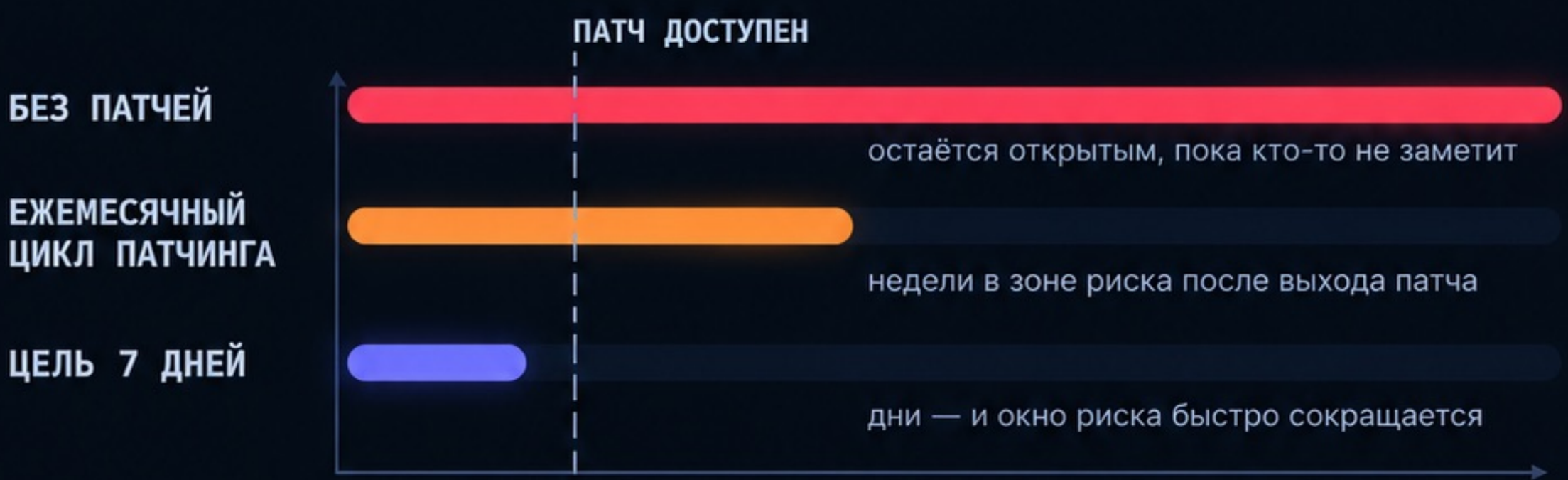
СЛОЙ 04 • 09/20

ENDPOINT

Ноутбуки, телефоны и серверы — это места, где код действительно выполняется. Большинство реальных инцидентов начинаются именно здесь, в первые минуты после запуска.



КАК ДОЛГО УЯЗВИМОСТЬ ОСТАЁТСЯ ОТКРЫТОЙ



Всё, что находится правее этой линии — это время, в которое вы осознанно остаётесь в зоне риска.

КЛЮЧЕВЫЕ КОНТРОЛИ НА ENDPOINT

Patch on a clock
Регулярный патчинг

Disk encryption
Шифрование дисков

Behaviour monitoring
Мониторинг поведения

No local admin
Минимальные права

Allow-listing
Разрешённые приложения и скрипты

ПРЕДОТВРАЩАЕТ

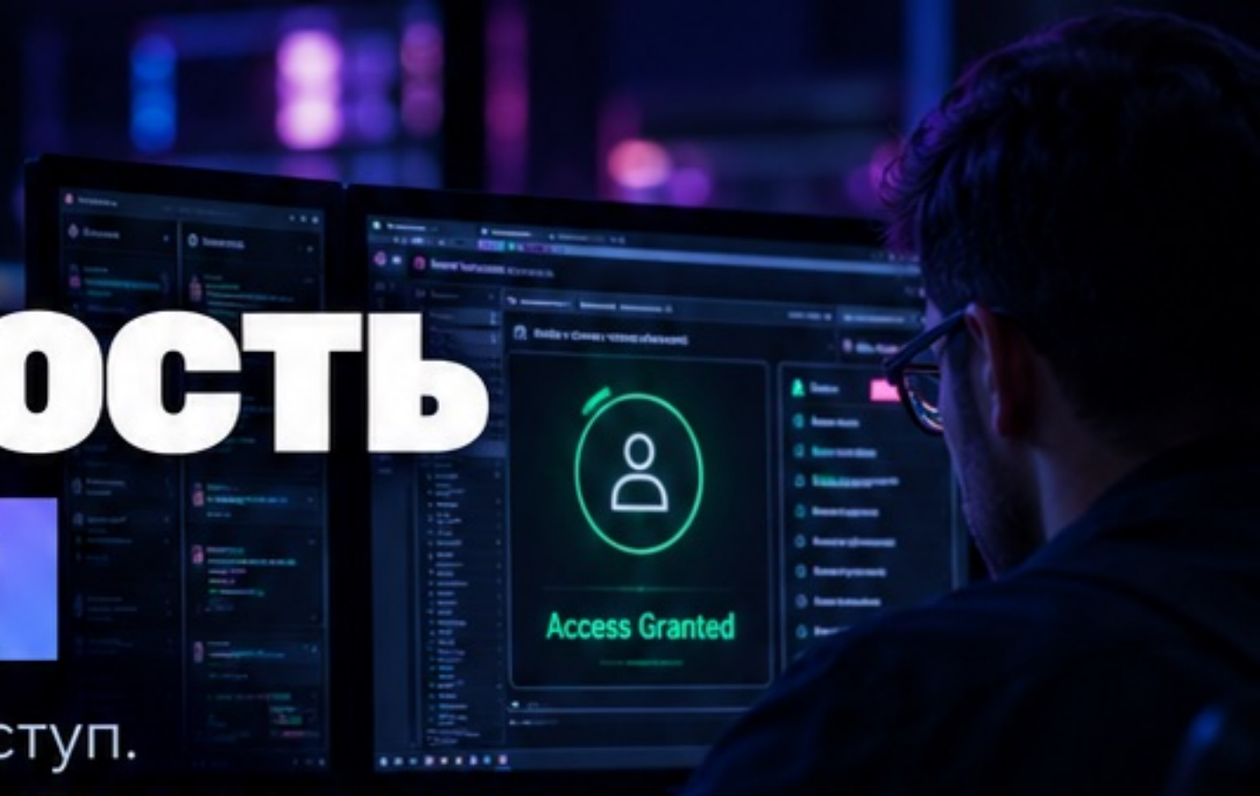
Известный malware и эксплуатацию уязвимостей, для которых уже есть **fix** (патч).

ВСЁ ЕЩЁ ПРОПУСКАЕТ

Новые уязвимости **(0-day)** или атакующего, использующего ваши же инструменты.

СЛОЙ 03 • 10/20

ИДЕНТИЧНОСТЬ И ДОСТУП



Кто вы, и к чему вам разрешён доступ. Как только у атакующего есть действующая учётная запись, большинство остальных слоёв перестаёт быть препятствием.

ЗАПРОС
кто-то запрашивает доступ

→

КТО?
проверка личности

→

К ЧЕМУ?
только нужные права (role rights)

→

НА КАКОЕ ВРЕМЯ?
ограничено по времени

→ **РАЗРЕШИТЬ**

СЛАБАЯ ПРОВЕРКА — ОТКАЗ И ЛОГИРОВАНИЕ

КОНТРОЛИ НА ЭТОМ СЛОЕ

MFA
Второй фактор

Минимальные права
Principle of least privilege

Доступ на время
Just-in-time access

Быстрый отзыв доступа
Fast offboarding

Логирование всех действий
Полный аудит

ПРЕДОТВРАЩАЕТ

Один украденный пароль и растущие привилегии.

ВСЁ ЕЩЁ ПРОПУСКАЕТ

Украденную сессию или пользователя, который одобрил поддельный запрос.

СЛОЙ 02 • 11/20

ПРИЛОЖЕНИЕ И ЛОГИКА

Код превращает запрос в действие. Каждое поле формы, каждая кнопка и каждый API-вызов — это потенциальный ввод от кого-то другого.

КАК ЗАПРОС СТАНОВИТСЯ ДЕЙСТВИЕМ

REQUEST
Пользователь отправляет данные

VALIDATE
Проверка входных данных

AUTHORIZE
Права и роли (role rights)

PROCESS
Бизнес-логика

ENCODE
Формирование ответа

RESPONSE
Данные уходят пользователю

ОТКЛОНЯЕМ НЕКОРРЕКТНЫЕ ДАННЫЕ

НЕТ ПРАВ — ФИКСИРУЕМ И БЛОКИРУЕМ

ПАТЧ НЕ РЕШАЕТ ПРОБЛЕМУ ЛОГИКИ

КЛЮЧЕВЫЕ КОНТРОЛИ ЗДЕСЬ

Проверка входных данных
Валидация и санитизация

Безопасная обработка
Корректное кодирование выходных данных

Проверки на уровне объектов
Контроль доступа к ресурсу, а не только к эндпоинту

Отслеживание зависимостей
Библиотеки и сторонние компоненты

Тестирование перед релизом
SAST / DAST и ручные проверки

ПРЕДОТВРАЩАЕТ

- Инъекции и некорректные данные
- Обход логики авторизации (broken access)
- Уязвимости в известных библиотеках

ВСЁ ЕЩЁ ПРОПУСКАЕТ

Логические ошибки:
реальные действия в порядке, которого вы не ожидали.

@lionsoulbatyshchikov

СЛОЙ 01 • 12/20

ДАННЫЕ

Это то, ради чего всё происходит. Если другие слои не срабатывают, именно этот слой определяет, будет ли инцидент дорогим или катастрофическим.



ТРИ СОСТОЯНИЯ, ТРИ ОТВЕТА

В ПОКОЕ

Зашифрованные диски, ключи хранятся отдельно.



В ПЕРЕДАЧЕ

Зашифровано в браузере и между серверами.



В ИСПОЛЬЗОВАНИИ

Держим минимум, маскируем чувствительное, фиксируем, кто читал.



И ОДНА КОПИЯ, КОТОРАЯ СПАСАЕТ ДЕНЬ

3 **копии данных**

основная, резервная, и ещё одна.

2 **разных типа хранения**

например, диск и облачное хранилище.

1 **копия офлайн**

недоступна для атакующих.

КЛЮЧЕВЫЕ КОНТРОЛИ НА ЭТОМ СЛОЕ

Шифрование везде
данные в покое и в передаче

Разделение ключей
ключи отдельно от данных

Минимизация данных
не храним лишнее

Офлайн резервные копии
защита от шифровальщиков

Контроль экспорта
уведомления о выгрузке

ПРЕДОТВРАЩАЕТ

Читабельные данные на украденном диске и тихое массовое копирование.

ВСЁ ЕЩЁ ПРОПУСКАЕТ

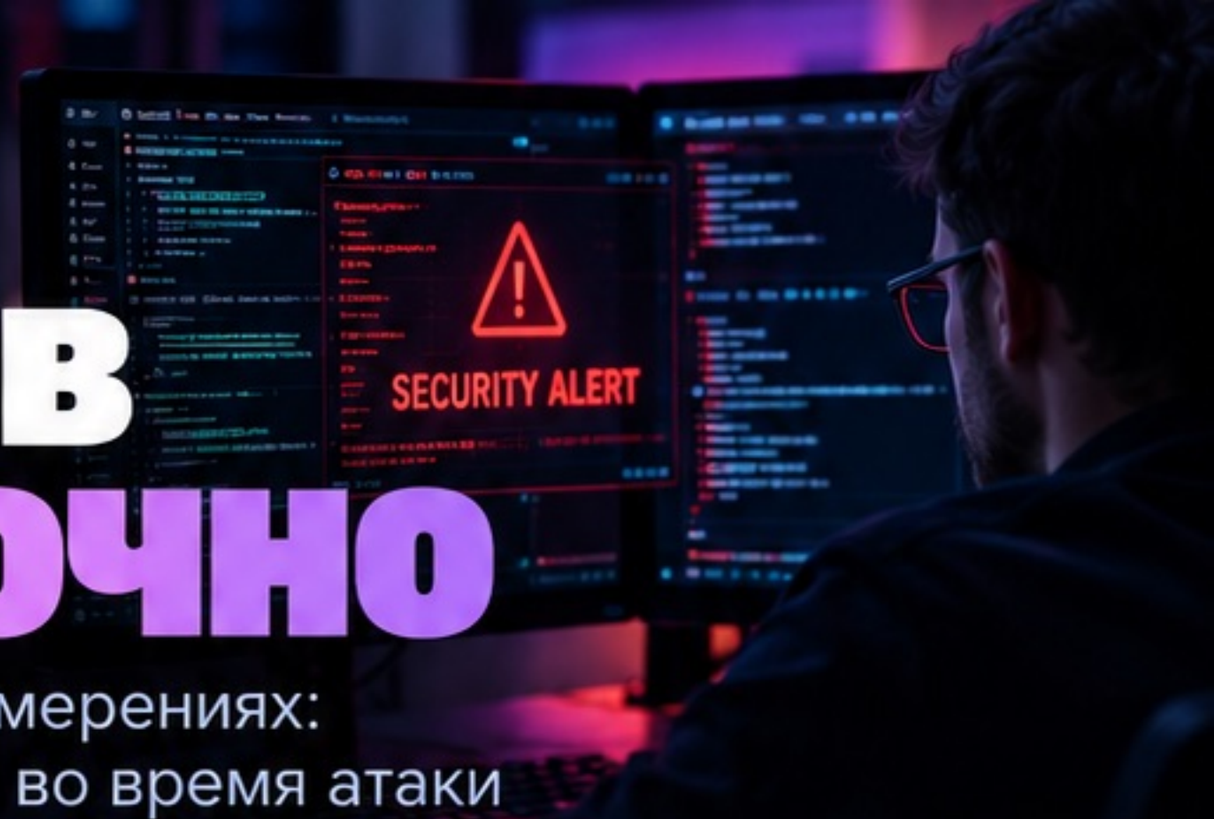
Действующую учётную запись, которая читает именно то, что ей положено.

@lionsoulbatyshchikov

СЛОЙ 02 • 13/20

ДВУХ СЛОЁВ НЕДОСТАТОЧНО

Глубина защиты работает в двух измерениях:
через слои и во времени. До атаки, во время атаки
и после — для каждого этапа нужны свои меры.



01 **СДЕРЖАТЬ** Сделать это дорогим

Видимость, камеры, предупреждения,
культура репорта.



02 **ПРЕДОТВРАТИТЬ** Не допустить

Патчи, second factors, запрет по умолчанию
(deny by default).



03 **ОБНАРУЖИТЬ** Заметить вовремя

Логи, которые реально читают,
и алерты на аномалии.



04 **РЕАГИРОВАТЬ** Ограничить ущерб

Изолировать хост, отозвать сессию,
заблокировать путь.



05 **ВОССТАНОВИТЬ** Вернуться и научиться

Поднять данные из бэкапа, устранить причину,
зафиксировать и задокументировать.



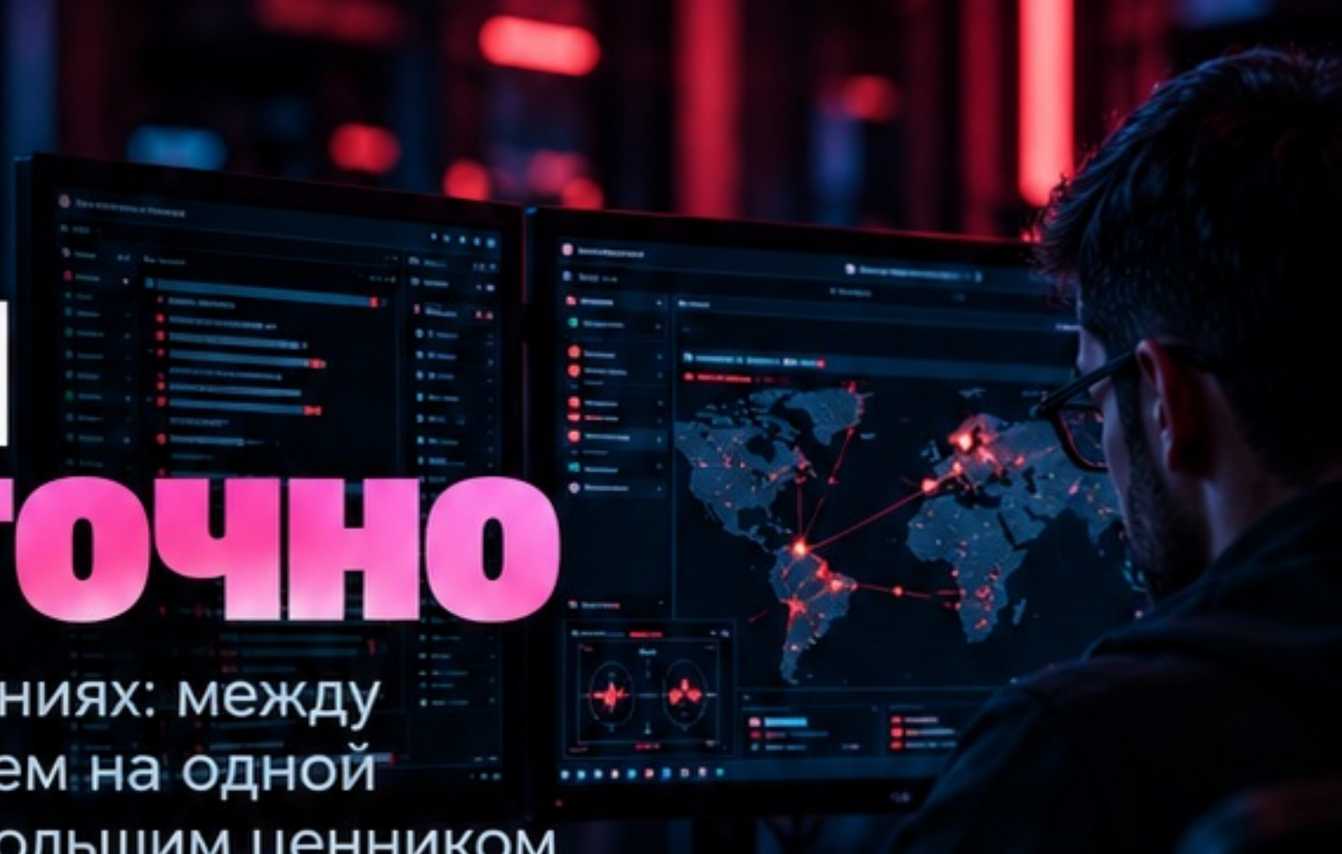
ПРОБЕЛ

Большинство останавливаются на первых двух шагах.
Если ничего не обнаружить и не отреагировать —
о компрометации расскажет кто-то другой.

@lionsoulbatyshchikov

СЛОЙ 01 • 14/20

ГЛУБИНЫ НЕДОСТАТОЧНО



Глубина работает в двух измерениях: между слоями и во времени. Пять систем на одной двери — это всего один слой с большим ценником. Постройте покрытие по всей цепочке, и реальные пробелы станут видны сразу.

СЛОЙ	ПРЕДОТВРАЩАЕТ	ОБНАРУЖИВАЕТ	РЕАГИРУЕТ
NETWORK Сетевой периметр и трафик	✓	—	—
ENDPOINT Устройства и рабочие станции	✓	◐	—
IDENTITY Учётные записи и права доступа	✓	—	◐
APPLICATION Приложения и бизнес-логика	◐	—	—
DATA Данные и хранилища	✓	—	◐

✓ РАБОТАЕТ ◐ ЧАСТИЧНО — НЕТ

КОЛОНКА ОБНАРУЖЕНИЯ ПОЧТИ ПУСТАЯ

ГЛАВНЫЙ ВОПРОС

Прежде чем покупать очередіной продукт, задайте себе: какой слой, какой тип и **что он обнаружит, что другие уже пропускают?**

@lionsoulbatyshchikov

СЛОЙ 01 • 15/20

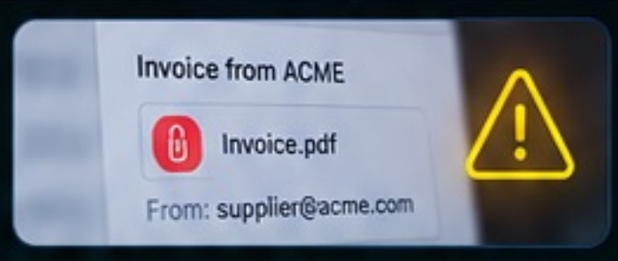
ОДНО ВТОРЖЕНИЕ, ШЕСТЬ ШАГОВ

Один и тот же атакующий, одна цель —
но теперь задействованы все слои.
Нет одного шага, который останавливает атаку.
Вместе они превращают её в сложную и шумную работу.

01 PEOPLE

Убедительное письмо с инвойсом.

Десять человек получают его, двое открывают.



ЧАСТИЧНО УДАЛОСЬ

02 ENDPOINT

Вложение пытается установить tool.

Срабатывает allow-listing, установка блокируется.

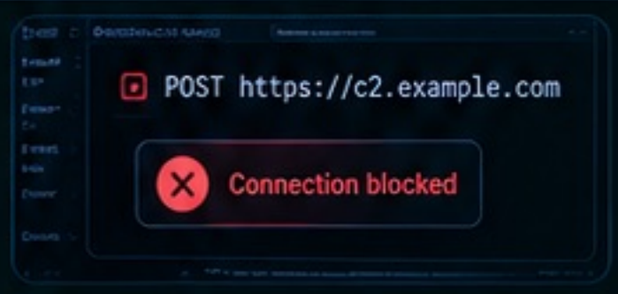


ЗАМЕДЛЕНО

03 NETWORK

Скрипт звонит “домой” за инструкциями.

Срабатывает egress filter,
генерируется alert.

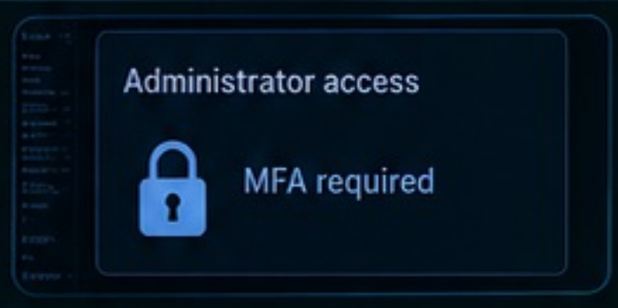


ОСТАНОВЛЕНО

04 IDENTITY

Попытка стать администратором.

Нет локального admin, дополнительно требуется второй фактор (MFA).



ОСТАНОВЛЕНО

05 NETWORK

Поиск серверного сегмента.

Сегментация не даёт установить соединение.

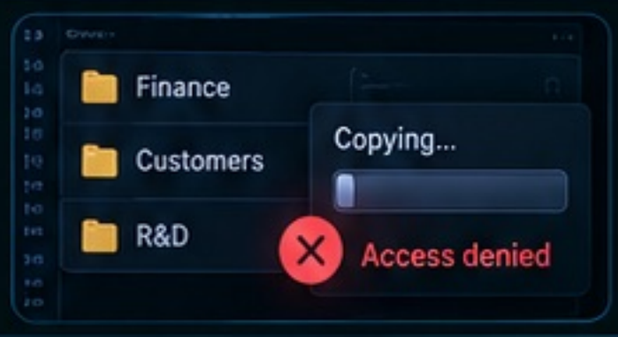


ОСТАНОВЛЕНО

06 DATA

Доступ к файловому шару и попытка копирования.

Данные зашифрованы, срабатывает alert на массовое копирование.



ОСТАНОВЛЕНО

КАК ЭТО ЧИТАТЬ

Это не реальные метрики, а иллюстрация. Смысл — в форме:
шесть отдельных возможностей заметить атаку, а не одна.

@lionsoulbatyshchikov

СЛОЙ 01 • 16/20

ЧЕТЫРЕ ЗАБЛУЖДЕНИЯ, В КОТОРЫЕ ЧАСТО ВЕРЯТ

Если от запомнили всего четыре вещи
из этого гайда — пусть это будут они.

МИФ 01

Больше инструментов значит больше глубины защиты.



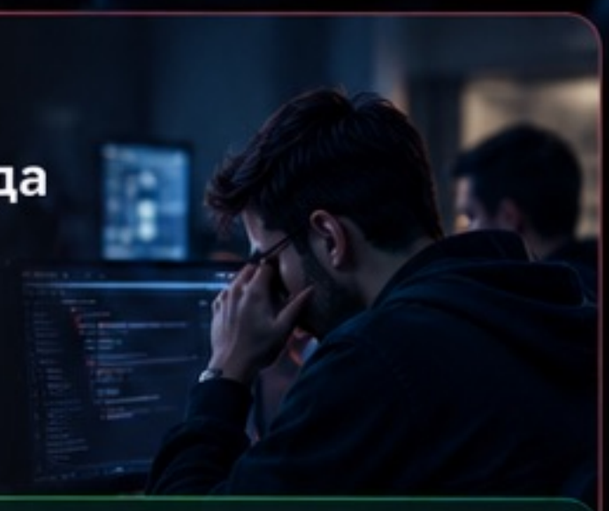
РЕАЛЬНОСТЬ

Часто это те же возможности, но за большие деньги.

Глубина — не в числе tools, а в правильном использовании.

МИФ 02

Небольшая команда не может сделать это эффективно.

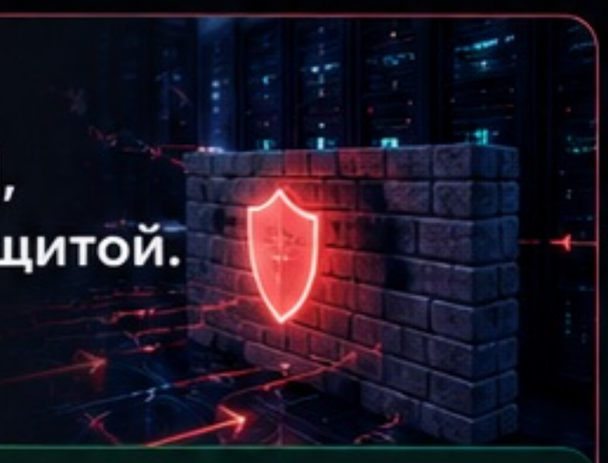


РЕАЛЬНОСТЬ

Second factors и регулярные backups — это уже два слоя, которые значительно повышают устойчивость, даже с небольшой командой.

МИФ 03

У нас есть firewall, значит мы под защитой.



РЕАЛЬНОСТЬ

Контроль, который нельзя мониторить — это не защита. Без логов, алертов и реакции вы не увидите, что происходит.

МИФ 04

Zero trust заменяет глубокую защиту.



РЕАЛЬНОСТЬ

Zero trust — это подход, который задаёт форму для слоёв защиты, но не заменяет их. Он усиливает то, что у вас уже есть.

ГЛАВНЫЙ ВЫВОД

Во всех этих заблуждениях есть одна общая ошибка:
люди считают, что нашли один слой,
а на самом деле это лишь часть большего.

@lionsoulbatyshchikov

СЛОЙ 01 • 17/20

ТРИ ПОДХОДА, ОДНА ЦЕЛЬ

Эти подходы часто рассматривают как альтернативы, но на самом деле они дополняют друг друга. Каждый отвечает на свой вопрос об атаке.

DEFENSE IN DEPTH

МНОГОСЛОЙНАЯ ЗАЩИТА



ПРЕДПОЛАГАЕТ

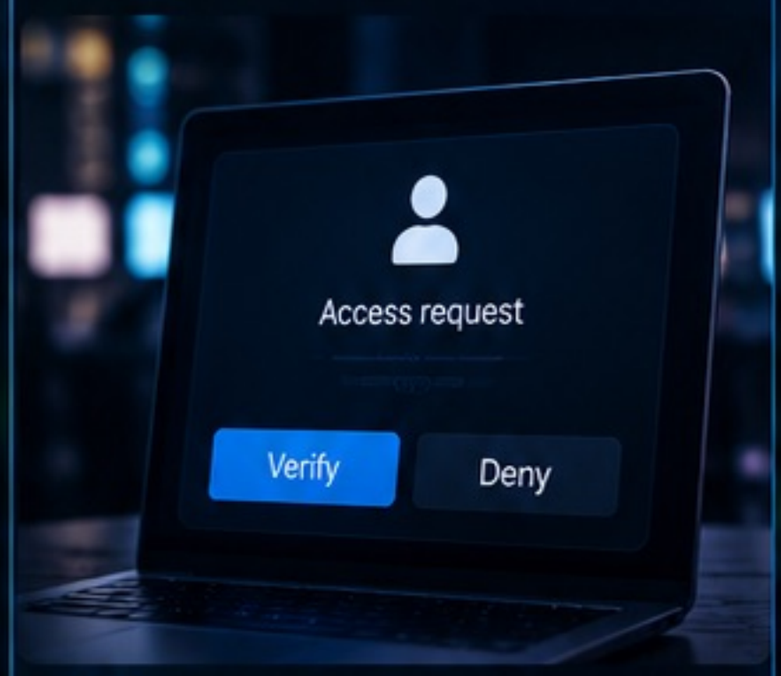
Любой отдельный контроль может быть обойден.

ПОЭТОМУ

Используем несколько разных контролей между атакующим и данными.

ZERO TRUST

НИКАКОГО АВТОДОВЕРИЯ



ПРЕДПОЛАГАЕТ

Сеть по умолчанию считается враждебной (hostile).

ПОЭТОМУ

Проверяем каждый запрос и его контекст, независимо от источника.

LEAST PRIVILEGE

МИНИМАЛЬНЫЕ ПРАВА



ПРЕДПОЛАГАЕТ

Любая учётная запись может быть скомпрометирована.

ПОЭТОМУ

Даем только минимум необходимых прав, на минимальное время, и забираем их обратно.

ГЛАВНАЯ ИДЕЯ

Глубина — это **форма**. Zero trust — это **правило** входа в слой. Least privilege — это **размер двери**, когда вы уже внутри.

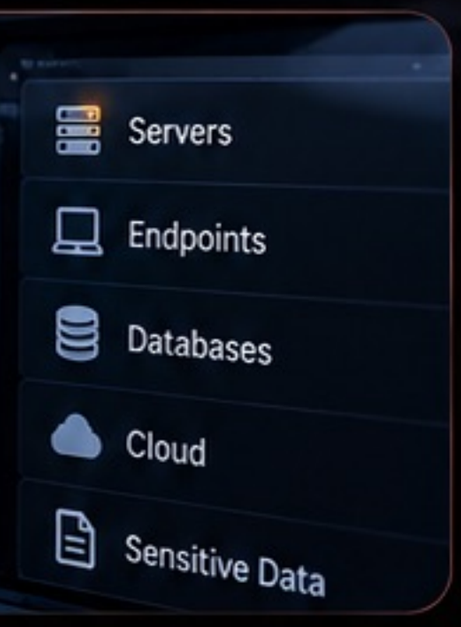
СЛОЙ 01 • 18/20

ПОСТРОЙТЕ ЭТО В ШЕСТЬ ШАГОВ

Подходит для компании, домашней лаборатории или одного ноутбука. Меняется только масштаб, а не логика.

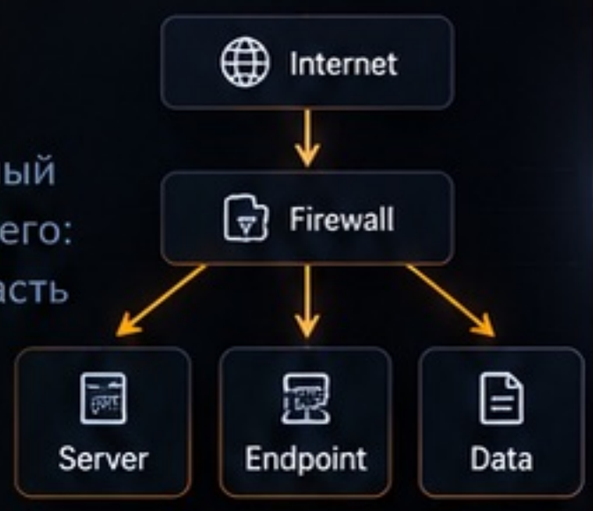
01 Определите, что защищаете

Нельзя защитить то, чего нет в списке: активы, данные, сервисы, ключевые процессы.



02 Постройте путь к ним

Нарисуйте реальный маршрут атакующего: как он может попасть к каждому слою (attack path).



03 Нанесите, что у вас есть

Отметьте для каждого слоя тип и конкретные контроли. Часто это выявляет неожиданные пробелы.



04 Найдите одиночные точки

Проверьте, что будет, если этот контроль исчезнет сегодня. Где останется прямой доступ (single point)?



05 Добавьте видимость, а не замки

Сначала логи и алерты. Пустая колонка в мониторинге важнее, чем еще один запрет.



06 Проверьте то, что построили

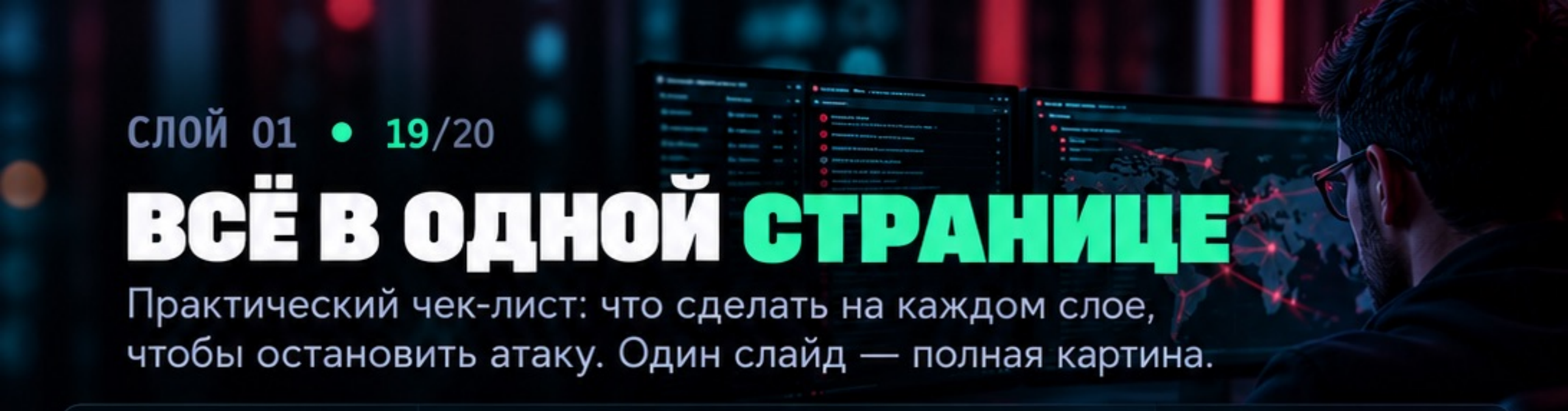
Восстановитесь из бэкапа, проведите небольшой drill, пройдите сценарий вместе с командой.



ГЛАВНАЯ МЫСЛЬ

Первый шаг ничего не стоит и занимает всего пару часов. Его почти никто не пропускает — потому что он мгновенно показывает, **где вы действительно уязвимы**.

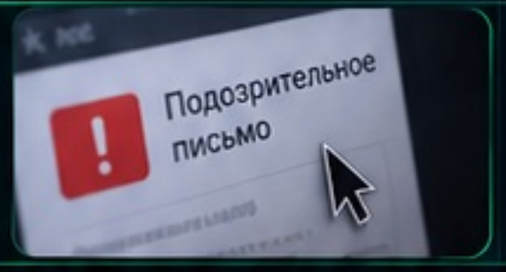
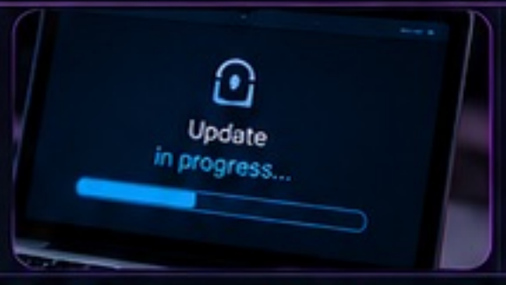
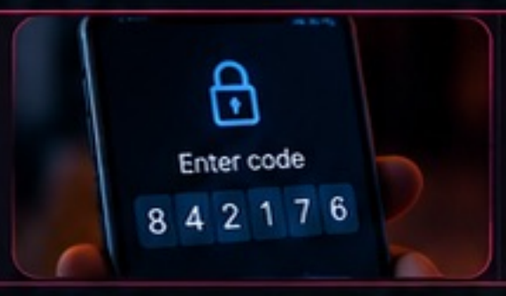
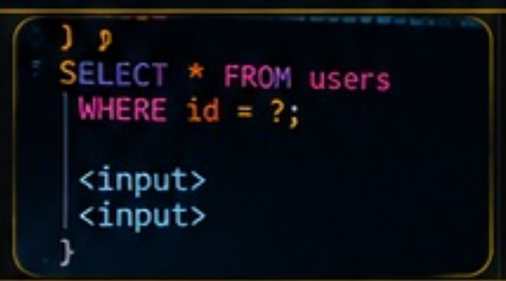
@lionsoulbatyshchikov



СЛОЙ 01 • 19/20

ВСЁ В ОДНОЙ СТРАНИЦЕ

Практический чек-лист: что сделать на каждом слое, чтобы остановить атаку. Один слайд — полная картина.

СЛОЙ	СДЕЛАЙТЕ В ПЕРВУЮ ОЧЕРЕДЬ		ЭТО ОСТАНАВЛИВАЕТ
PEOPLE Люди	Настройте **reporting** и короткие регулярные тренинги.		Меньше случайных кликов и успешных фишинговых атак.
PHYSICAL Физическая безопасность	**Бейджи**, сопровождение посетителей, закрытые стойки и помещения.		Предотвращает несанкционированный физический доступ (walk-in access).
NETWORK Сеть	**Запрет** по умолчанию, сегментация (zones) и **egress filtering**.		Ограничивает перемещение атакующего и боковые движения (lateral movement).
ENDPOINT Рабочие станции и устройства	**Патчи** вовремя, шифрование, отключение локального админа.		Снижает риск известного malware и эксплуатации уязвимостей.
IDENTITY Учётные записи и доступ	**MFA,** минимум прав (least privilege), быстрое отключение доступа.		Краденые пароли и скомпрометированные учётные записи не дают полного доступа.
APPLICATION Приложения	**Валидация** входных данных, кодирование выхода, проверка каждого объекта.		Блокирует инъекции (injection) и несанкционированный доступ.
DATA Данные	**Шифрование**, принцип **keep less**, правило **3-2-1** для бэкапов, алерты на экспорт.		Даже при инциденте данные остаются защищёнными, а утечка заметна сразу.

ГЛАВНАЯ ИДЕЯ

- Разные типы контроля останавливают **одни и те же атаки**.
- Каждому слою нужен свой **механизм наблюдения**.
- Непроверенный слой — это лишь **видимость защиты**.

@lionsoulbatyshchikov