

ГРАФЫ ЗНАНИЙ В ИТ, ИИ И КИБЕРБЕЗОПАСНОСТИ

WEEK 1: ВВЕДЕНИЕ, КИБЕРВЕРТИКАЛЬ
И ПОСТАНОВКА ПРОЕКТНОГО РЕЗУЛЬТАТА

 	ПРОЕКТ: Ковчег знаний МГУ
	WORKSTREAMS: WS-1 (Данные) + WS-2 (Граф)
	UNIT: Введение и регламенты
	ARTIFACT: M5-A1



КИБЕР-СЛОЙ ПРОЕКТА: ДЛЯ КОГО МЫ СТРОИМ ГРАФ?

Потребители модели знаний и их ключевые задачи



RADAR/SCOPE

SOC (Security Operations Center)

Контекстуализация алертов.
Не просто «что упало», а с чем это связано и каков приоритет.



SHIELD & BOLT

CSIRT/CERT (Incident Response)

Расследование цепочек событий, атрибуция атак и реконструкция инцидента.

**Граф отвечает на вопросы:
«Что затронуто?» и «Где закономерность?»**



GEAR & LOCK

DevSecOps

Связь уязвимостей (CVE) с компонентами ПО, зависимостями и контрмерами.



TREND CHART

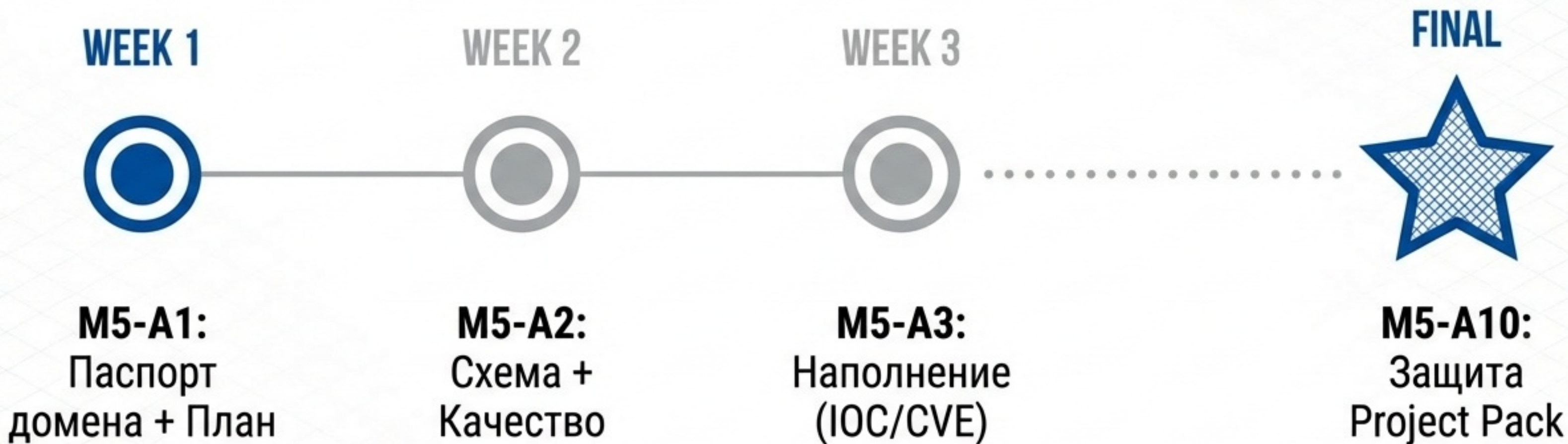
Management

Объяснимость решений (Explainability) и оценка рисков на основе данных.

ИНЖЕНЕРНЫЙ КОНТРАКТ

Единица результата — проверяемый артефакт

ЗОЛОТОЕ ПРАВИЛО: НЕ СДАН АРТЕФАКТ — НЕДЕЛЯ НЕ ЗАСЧИТАНА



Курс построен на производстве инженерных артефактов, а не на потреблении контента.

ПРАВИЛА ИГРЫ: КРАСНЫЕ ЛИНИИ (SAFETY & ETHICS)

ТРЕБУЕТСЯ (REQUIRED)



- Работа только в изолированном учебном контуре (Lab)
- Использование синтетических или обезличенных данных
- Полное соблюдение законодательства РФ
- Фиксация источников и лицензий

ЗАПРЕЩЕНО (FORBIDDEN)



- Любые атаки на внешние системы
- Использование реальных ПДн (Персональных Данных)
- Работа с боевыми логами (Production) без разрешения
- Использование реальных секретов/паролей

КУЛЬТУРА ИНЖЕНЕРИИ ДАННЫХ: ПРОСЛЕЖИВАЕМОСТЬ

В кибер-аналитике факт без источника — это шум



ИСТОЧНИК (SOURCE)

URL, отчет, фид
(Source Register)

ВЕРСИЯ (VERSION)

Дата доступа, хэш,
версия файла

ТРАНСФОРМАЦИЯ

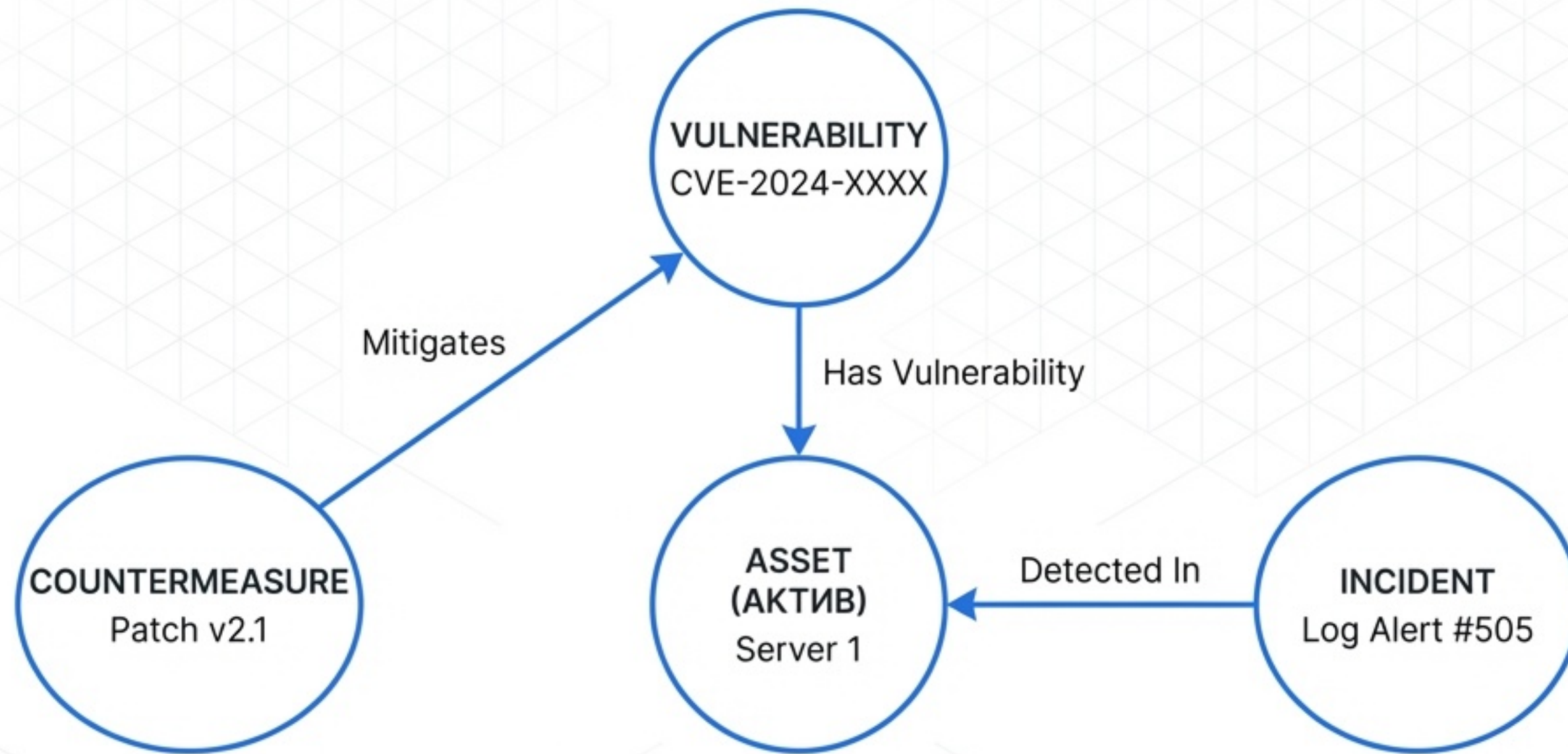
Скрипт загрузки / ETL

РЕЗУЛЬТАТ

Узел или связь
в графе

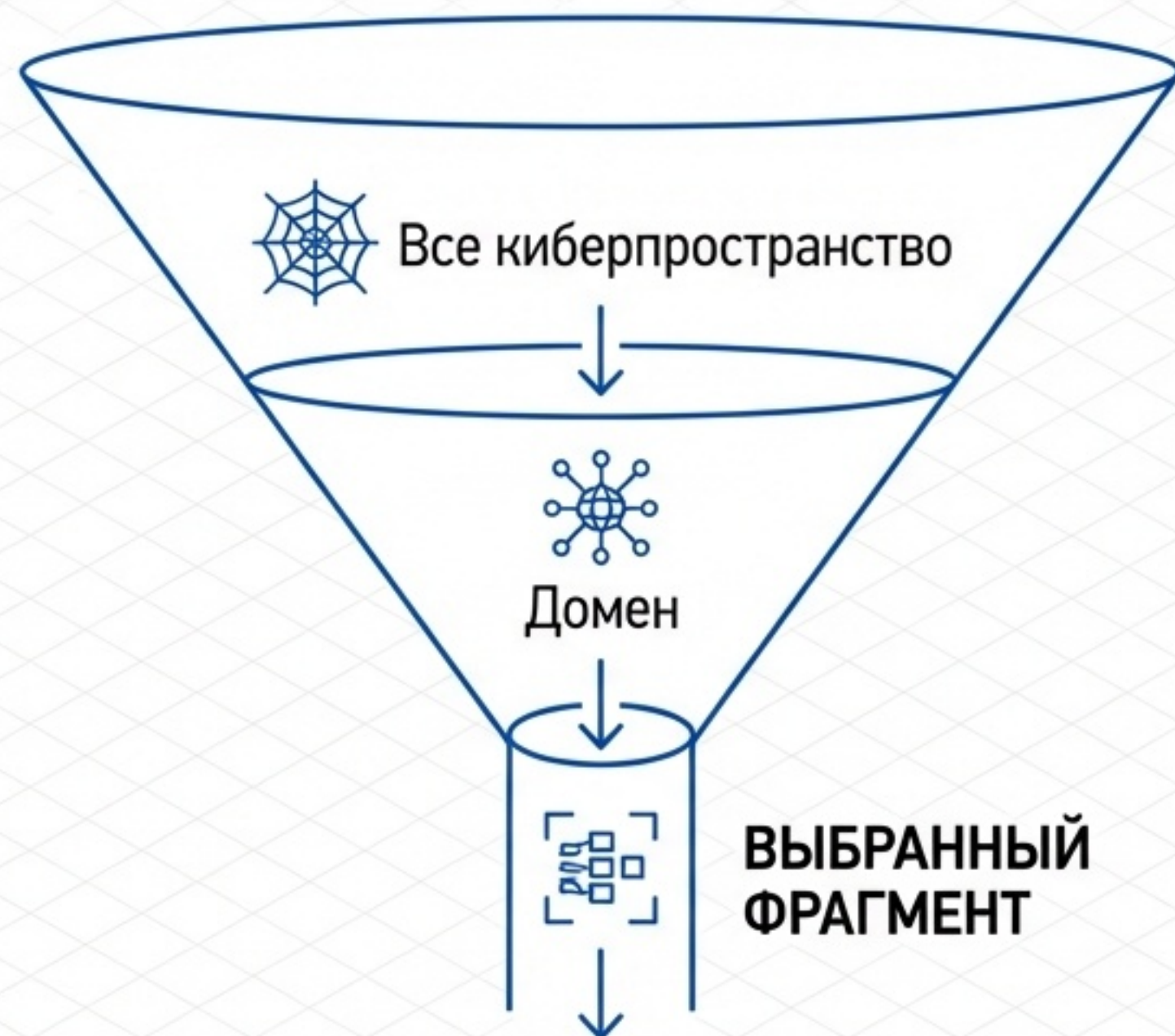
Требование: Любое утверждение в графе должно быть трассируемо до конкретной версии источника.

МЕНТАЛЬНАЯ МОДЕЛЬ: КАК ВЫГЛЯДИТ КИБЕР-ГРАФ?



Мы моделируем семантические связи, чтобы ответить на вопрос:
«Какие активы под угрозой из-за отсутствия патча?»

ВЫБОР ФРАГМЕНТА ДОМЕНА: КРИТЕРИИ УСПЕХА



Checklist выбора

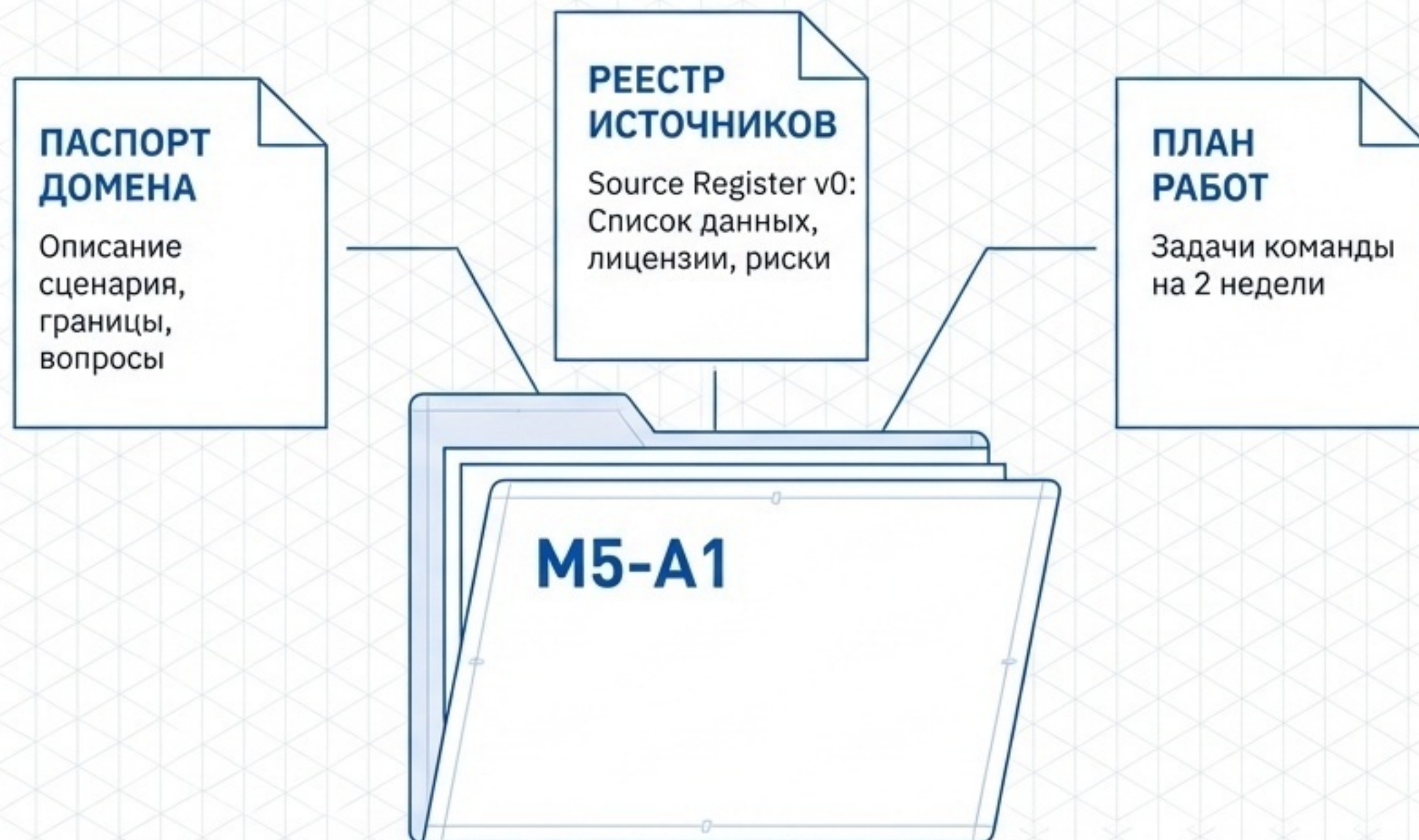
- ☒  **ИЗМЕРИМОСТЬ:** Можно ли показать демо за 3-5 минут?
- ☒  **ДАННЫЕ:** Есть ли минимум 3 легальных открытых источника?
- ☒  **ГРАНИЦЫ:** Четко ли определено, что входит (IN), а что нет (OUT)?
- ☒  **ВОПРОСЫ:** Можно ли сформулировать 3 проверяемых Competency Questions?



Не пытайтесь смоделировать «всё». Лучше глубоко проработать узкий сценарий.

АРТЕФАКТ WEEK 1: M5-A1

Состав пакета для сдачи



Цель:

Заложить фундамент. Без этих документов невозможно построить схему (Week 2).

КОМПОНЕНТ 1: ПАСПОРТ ДОМЕНА И ВОПРОСЫ

СТРУКТУРА ПАСПОРТА

 **Целевой сценарий:** Кто пользователь?
(напр., Junior SOC Analyst)

 **Границы:** Таблица 2x2
(Входит / Не входит)

ВХОДИТ	НЕ ВХОДИТ

COMPETENCY QUESTIONS (CQ)

Вопросы, на которые должен отвечать граф.

 **Плохой пример:** «Что такое вирус?»
(Это справочник, а не граф)

 **Хороший пример:** «Какие активы затронуты CVE-2024-XXXX и не имеют патча?» (Требует связи данных)

КОМПОНЕНТ 2: РЕЕСТР ИСТОЧНИКОВ (SOURCE REGISTER)

Основа соблюдения правил ИБ и воспроизводимости

 SOURCE ID (Unique Code)	 TYPE (Фид, Отчет, Датасет)	 ACCESS / LICENSE (Открытая, CC-BY, Требуется регистрации)	 DATA FIELDS (IP, Hash, CVE)	 QUALITY RISK (Устаревание, неполнота)
SRC-001	Фид	Открытая (CC-BY-SA)	IP, Port, Protocol	Высокий (Устаревание 24ч)
SRC-002	Фид	Открытая (CC-BY-SA)	IP, Port, Protocol	Высокий (Устаревание 24ч)
...	...	...	...	...

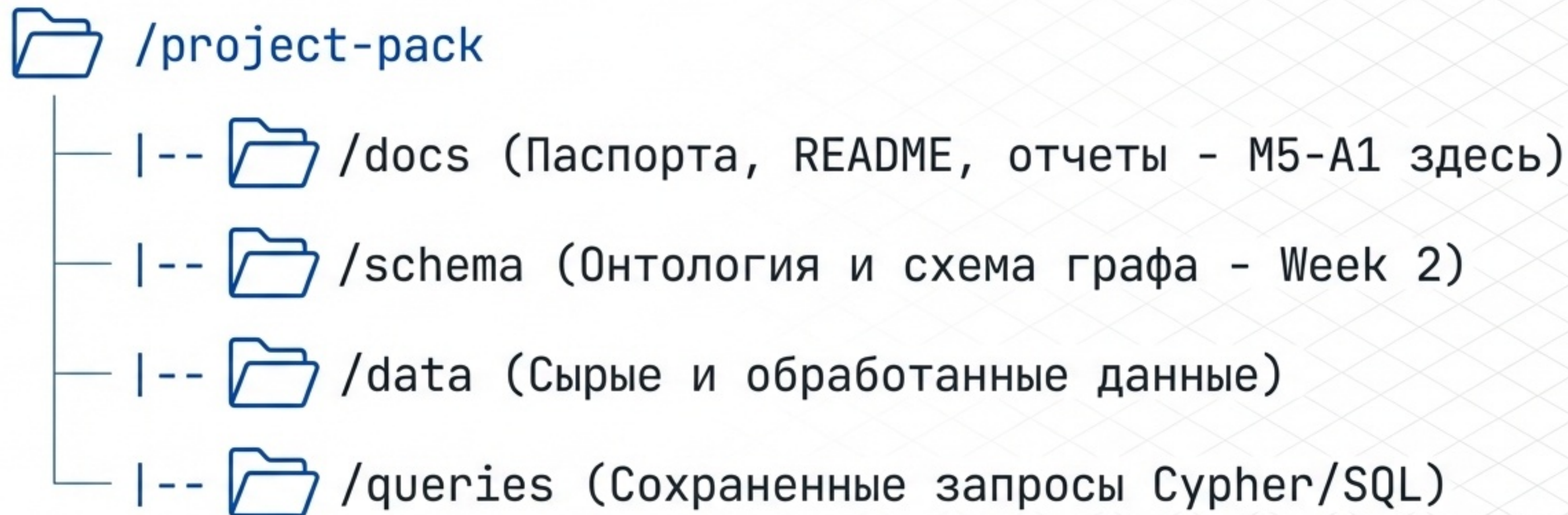
MINIMUM

3

Sources required for start

ТЕХНИЧЕСКАЯ СРЕДА: PROJECT PACK

Стандарт структуры репозитория



Создать репозиторий с этой структурой необходимо сейчас.

DEFINITION OF DONE (DoD)

Критерии приемки Week 1

LAUNCH CHECKLIST

- ☐ Границы домена заданы и не противоречат сценарию
- ☐ **10 Entities / 10 Relations** (Draft)
- ☐ **3 Competency Questions**
- ☐ Source Register **>= 3 источника** с лицензиями
- ☐ Артефакт загружен в Project Pack / LMS

IMMEDIATE ACTION

Заполнить Worksheet → Сделать 2-минутный питч → Пройти Intro Quiz