PHDays 2025: ИЦ

Алексей Синадский

30.05.2025, митап ИЦ

Лужники

CYBERARENA

КИБЕРАРЕНА

Бизнес-доклады, партнерские зоны
Business talks and partner zones

- R **Регистрация** Registration
- 11 **Зал 11 «Братья Райт»** Wright Brothers Hall 11
- 12 **Зал 12 «Тьюринг»** Turing Hall 12
- 13 **Зал 13 «Гальвани»** Galvani Hall 13
- 14 **Зал 14 «Маркони»** Marconi Hall 14
- 15 **Зал 15 «Морзе»** Morse Hall 15
- 16 **Зал 16 «Эдисон»** Edison Hall 16
- 17 **Зал 17 «Якоби»** Jacobi Hall 17
- 18 **Зал 18 «Королев»** Korolev Hall 18
- 19 **Выставка партнеров** Cyber expo
- 20 **Арена «Ломоносов»** Lomonosov Arena

CYBERHUB

КИБЕРХАБ

Технические доклады, воркшопы, Standoff
Technical talks, workshops, and Standoff

- R **Регистрация** Registration
- 21 **Зал 21 «Лавлейс»** Lovelace Hall 21
- 22 **Зал 22 «Горохов»** Gorokhov Hall 22
- 23 **Зал 23 «Да Винчи»** Da Vinci Hall 23
- 24 **Зал 24 «Шеннон»** Shannon Hall 24
- 25 **Зал 25 «Попов»** Popov Hall 25
- 26 **Зал 26 «Бэббидж»** Babbage Hall 26
- 27 **Positive Labs**
- 28 **Конкурсы PHDays** PHDays competition
- 29 **Positive Talent Spot**
  Место для общения с экспертами в ИТ и ИБ и обсуждения карьерных перспектив
  The place to network with IT and information security experts and discuss career prospects
- **Standoff**

Присмотрел доклад?

- 3 дня, параллельно 20+ залов

Зал 21 «Лавлейс» | Зал 22 «Горохов» | Зал 23 «Да Винчи» | Зал 24 «Шеннон»

Зал 25 «Попов» | Зал 26 «Бэббидж» | Лекторий Positive Labs | Standoff

Научпоп-сцена «KULIBIN» | Education Hub

Арена «Ломоносов» | Пресс-центр | Зал 11 «Братья Райт» | Зал 12 «Тьюринг» | Зал 13 «Гальвани»

Зал 14 «Маркони» | Зал 15 «Морзе» | Зал 16 «Эдисон» | Зал 17 «Якоби» | Зал 18 «Королев» | Пространство киберустойчивости Innostage

Время	Зал	Доклад
22.05		
12:00-13:00	Лавлейс	Как ломают DeepSeek и как ИИ ломает нас
13:00-13:50	Горохов	Apache Arrow: быстрее, ниже, сложнее
14:00-14:50	Горохов	Как мы приручали утку: работа с данными в X раз быстрее без магии и шаманства
15:00-16:00	Шеннон	Знай свой IoT: как ML-профилирование раскрывает атаки
15:00-16:00	Лекторий PT	(нет) Не стой под стрелой: безопасность систем промышленного дистанционного управления
15:30-15:45	Тьюринг	(нет) Что важно для защиты умных многоквартирных домов
16:00-16:50	Горохов	Как заставить тормозить ClickHouse
Куда-то пропал из программы		(мб) Как мы поймали актуальную угрозу после 1000 и 1 фолза на мемах «это база» и «слома
19:00-19:15	Шеннон	Применение легковесных LLM в аналитических задачах ИБ
23.05		
10:35-11:05	Королёв	LLM и агенты: разгоняем SOC
10:55-11:35	Тьюринг	Современные реалии проектирования и построения сетевой инфраструктуры
11:05-11:35	Королёв	AutoML threat detection: повышаем уровень автономности SOC
11:35-12:05	Королёв	Как мы делаем near-real-time защиту в Яндекс Облако: AI в процессах и технологиях
13:00-13:50	Да Винчи	Усиление облачной безопасности. Используем CSPM для нужд SOC
13:00-14:00	Лавлейс	Токены доступа и API gateway: как обеспечить безопасность запросов
13:45-14:00	Кололёв	Детектирование SSH-туннелей на основе системных вызовов от процесса демона SSH (sshd
14:00-14:50	Горохов	Централизованное управление распределенным файрволом
14:00-15:00	Кибергород	(мб, скорее нет) Кто такой этот ваш Искусственный Интеллект? Воркшоп
14:30-14:45	Эдисон	Как с помощью LLM выявлять реальные уязвимости LLM-приложений
15:00-16:00	Лавлейс	Источники данных для фаззинга API веб-приложений
15:00-16:00	Бэббидж	Развитие трейсинга в hh.ru. От Cassandra и OpenTelemetry до Vector и ClickHouse
15:00-15:50	Горохов	Что вы делаете не так с Elasticsearch с инженерной стороны
15:00-15:15	Эдисон	Как поймать атакующих на их ошибках
15:30-16:00	Королёв	IDFW: как заблокировать атаку везде и сразу
15:30-19:30	Гальвани	(мб) LLM в повседневной деятельности специалиста по ИБ; воркшоп
16:00-16:50	Да Винчи	Легитимные C2: как популярные сервисы работают на хакеров
16:40-17:20	Тьюринг	Харденинг сетевой инфраструктуры
17:30-18:15	Эдисон	Бизнес-разведка методами OSINT
18:00-18:40	Тьюринг	Контроль конфигурации сетевого оборудования. Как обеспечить?
24.05		Как мы изменения в сети валидировали
12:30-13:20	Горохов	VS Code: выжимаем все из нашей IDE — и даже больше
14:00-15:00	Да Винчи	Обеспечение конфиденциальности данных при разработке ML-моделей с использованием те
14:30-14:45	Тьюринг	Инвентаризация Windows посредством SSH
15:00-15:50	Горохов	Поиск аномалий с использованием Python: от теории к практике
16:00-17:00	Да Винчи	SDRcraft: искусство радиоэлектронной борьбы
	Kulibin (научпоп	(скорее, нет) Моделируя будущее: цифровые двойники
17:00-18:00	Шеннон	От яхт до рутинга: эксплуатация уязвимостей IoT для полной компрометации устройств

Доклады

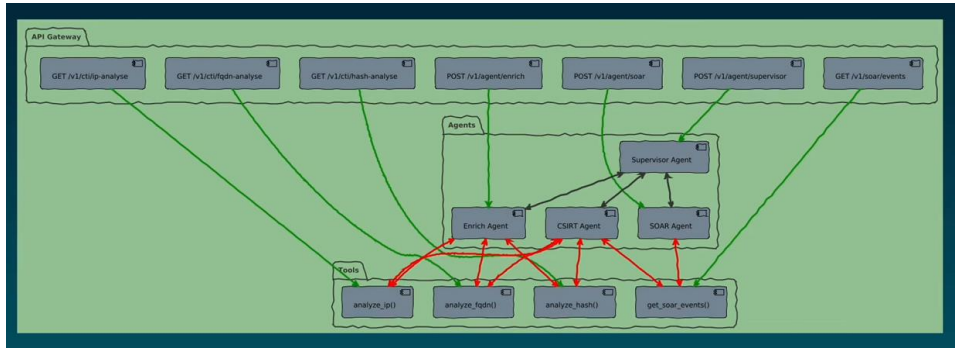
Программа: https://phdays.com/forum/program/
Записи: https://phdays.com/forum/broadcast/

Как ломают DeepSeek и как ИИ ломает нас

- Масалович ☹
- Сохранять, пока есть
- Применение – быстрый анализ решений конкурентов
- Сеть Колмогорова-Арнольда. Подбор f(x)
- Роевой ИИ. Социальные функции
- Модель Барабаши-Альберт, безмасштабные сети

доклад

LLM и агенты: разгоняем SOC

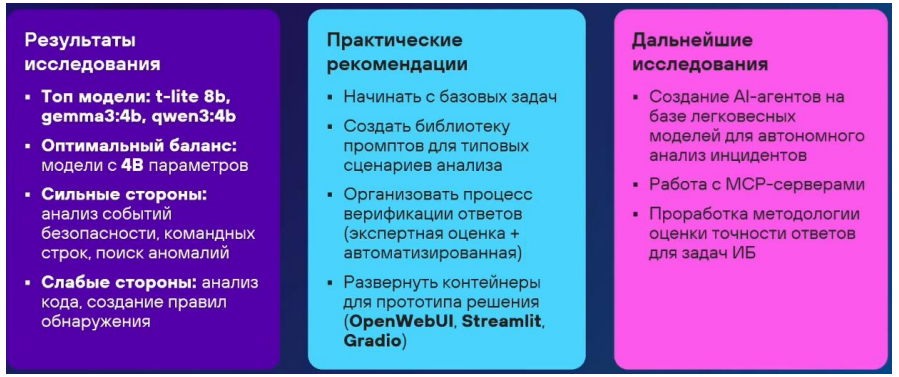


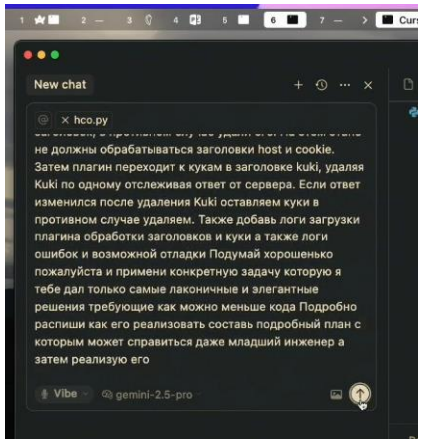
- В целом, работает, если не плоские чаты. Определить роль, инструменты, задачу
- Результат – Few-Shot для исследования экономит до 25% времени аналитика
- Рекомендации
  - Температура в 0, чтобы стабильно отвечать на одни и те же вопросы
  - Выбор модели: смотреть разные, не обязательно самые крутые
  - Промпт. Подавать корректные вопросы, формализовать ответы (что хочется получить)
  - Делать тесты с вопросами. Валидация входа/выхода - как минимум, на уровне http.
  - Мониторинг. LangSmith, Grafana
  - При внедрении явно отключать дебаг
  - Сбор диалогов и оценок
  - Использовать чистые данные, не обучать на синтетике, иначе через поколения будет хуже.

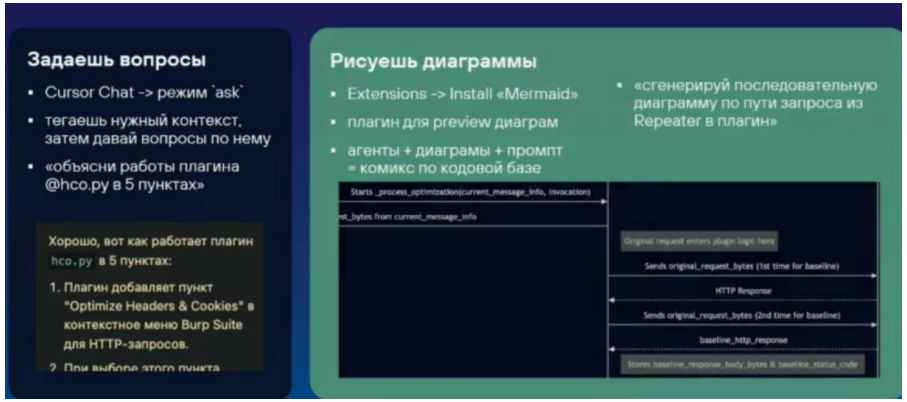
доклад

Легковесные LLM для аналитики [доклад]
Голос куратора: создаем плагин для Burp Suite без клавиатуры [доклад]

- Легковесные LLM для аналитики
  - Легковесные - до 8B
  - Отдельные задачи решают
  - С техническими задачками сложности
  - Выбор: T-lite, Gemma3, Qwen
- LLM в IDE
  - Лайв-кодинг в прямом эфире
  - Идея: не давать LLM свободы в фантазии, только реализация
  - LLM – «терпеливый джун»
  - CursorIDE + Gemini2.5Pro + WhisperFlow
  - Основной совет: менять чаты, хранить контекст
  - uithub.com – генератор исходников для LLM
    - (описание файлов из репозитория)

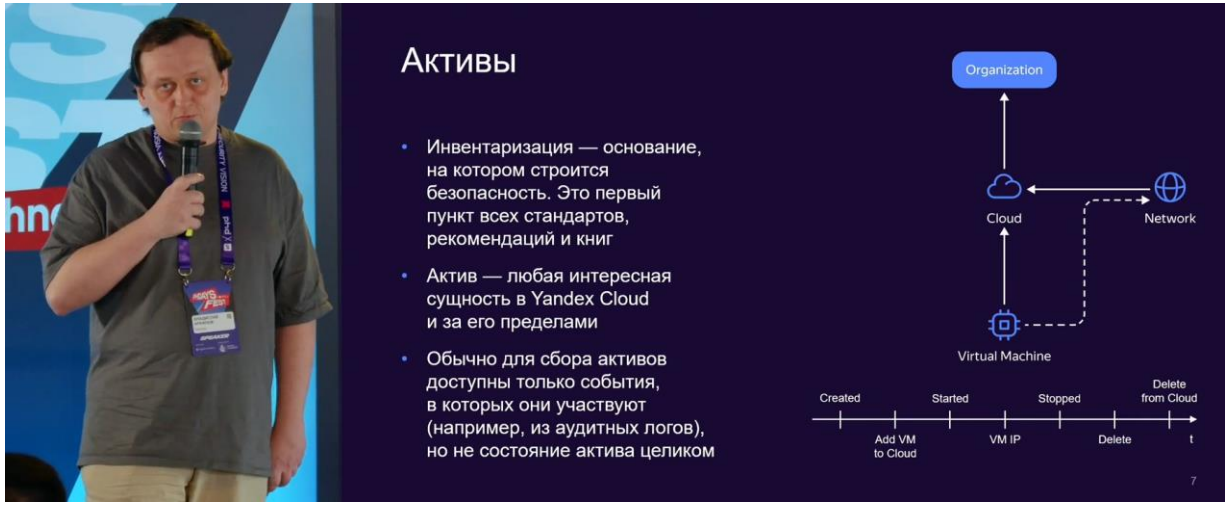


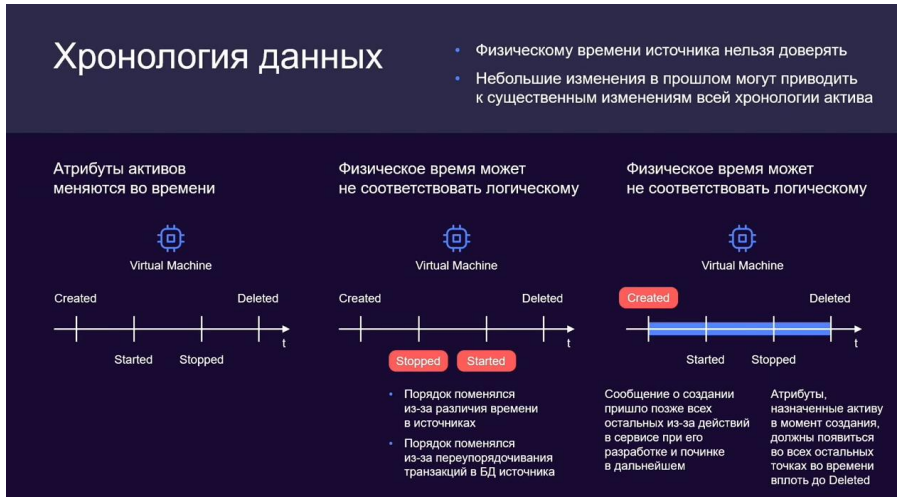




Как мы делаем near-real-time защиту в Яндекс Облако: AI в процессах и технологиях

- Начинать с инвентаризации (расширенная категоризация UDV NTA?)
- Хранить базу данных об активов с хронологией
- Полезно описывать изменения (+функция DATAPK Version Control?)





доклад

AutoML threat detection: повышаем уровень автономности SOC

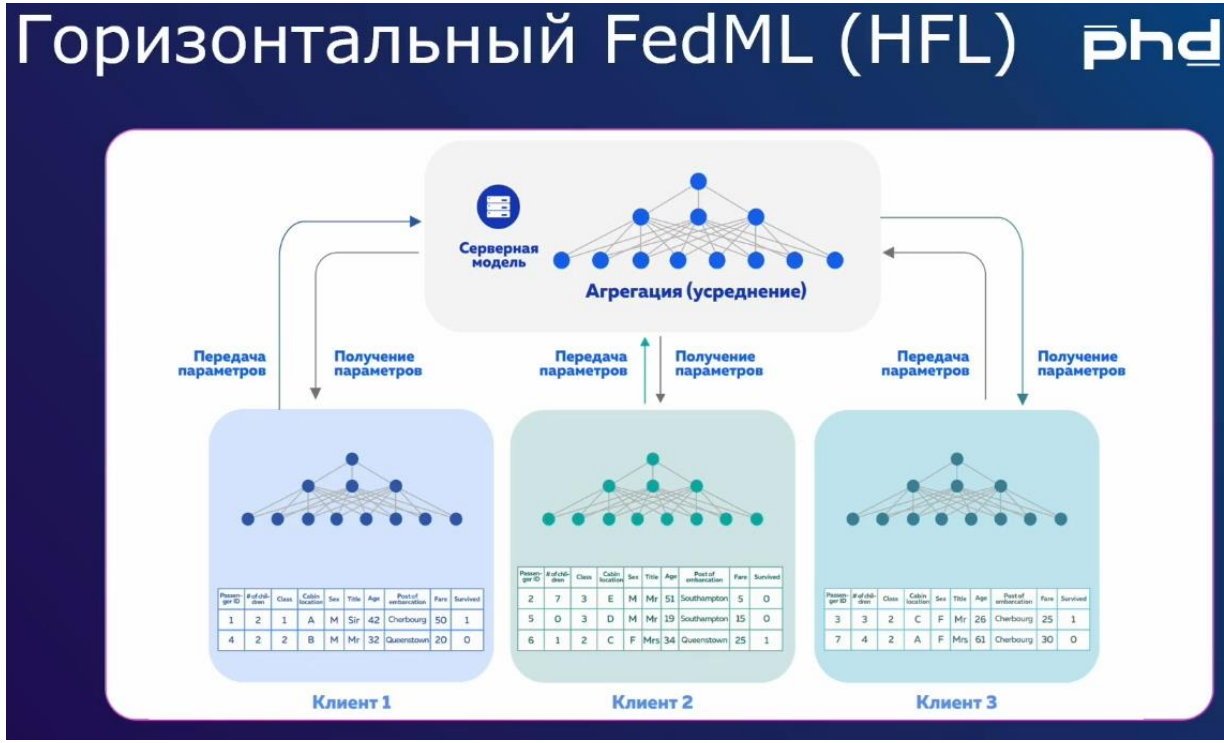
- Правила - ML - LLM
- Со структурированными данными ML пока помогает
  - Weak learning: взять правила, разметить большой датасет, использовать
- MLops -> AutoML -> AI ассистент
- ML-инженеры нужны, в основном, доменные
- Подробнее в рассказе Николая

доклад

FedML (aka Обеспечение конфиденциальности данных при разработке ML-моделей с использованием технологии федеративного обучения и криптографических методов)

[доклад]

- Как установить, кто самый богатый в комнате человек, не раскрывая состояние.
  - Горизонтальный FedML (HFL). Разные сущности, одинаковые признаки. Разные больницы.
  - Вертикальный FedML (VFL). Разные признаки, но пересекающие признаки.
- Чтобы нельзя было восстановить сущности из градиентов, используется гомоморфное шифрование. Пока могут только линейные преобразования. Полиномы не могут.
- Защиты от Poison-атак (отравления данных) пока нет.
- Идея применения в UDV: FedML для дообучения на отдельных производствах. Отдавать с логами эмбеддинги или градиенты. Снижение эффекта дрейфа данных.



Знай свой IoT: как ML-профилирование раскрывает атаки

- Выучивают IoT-устройства 26 фиксированных типов
  - Определять тип устройств ещё не умеют
- Выявление атак – но все связаны с ростом трафика
  - мб есть простые методы?
- Датает - CIC IoT 2022 (Канадский университет)
- Список признаков опубликован: GitHub
- Отдельные модели для выявления и классификации атак
- Лаборатория И.В. Котенко
- Дмитрий Левшун

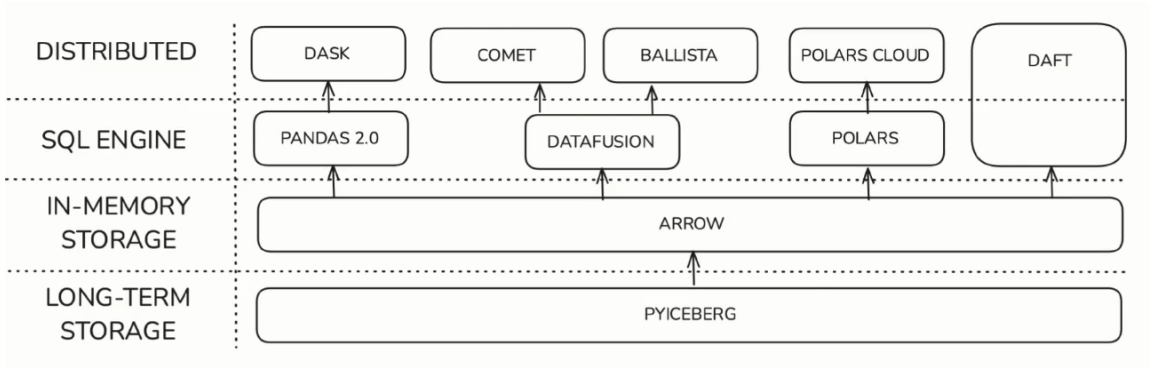
https://github.com/levshun

доклад

Про хранение данных:

Как мы приручали утку: работа с данными в X раз быстрее без магии и шаманства [доклад]

Apache Arrow: быстрее, ниже, сложнее [доклад]



- Хранение
  - Для хранения (120ГБ/час с одного) используют S3
  - S3 - проблемы от 100млн файлов; решения:
    - делать Parquet с одной тяжёлой колонкой (оверхед 1 байт на строку, в Pandas 57 при объекте)
    - Долговременное хранение: Pyiceberg
  - DuckDB - аналог SQLite для аналитических данных. In-process, не имеет зависимостей (всё в одной репе); так работает PT
- Чтение: Arrow
  - Недостатки: нет SQL-оптимизатора, только обработка примитивов. Поэтому Arrow встраивается в качестве compute.
  - DataFusion - SQL-движок для Arrow
  - Apache Arrow - произвольный доступ и прочее (не читать тяжёлую колонку, пока не прочитали остальное);
  - Arrow Scanner - экономия ОЗУ
- Обработка:
  - DataFusion Ballista - распределённые вычисления для DataFusion
  - Polaris - самый быстрый вариант обработки данных на одном узле.
    - Два режима выполнения: сразу как в Pandas и lazy как в Spark
    - Оконные функции в Polars работают неправильно. Пока довели до ума только примитивы.
  - 2022: появился DAFT. Как Polars, только умеет в распределённость. Создавался под ML. Появились оконные функции

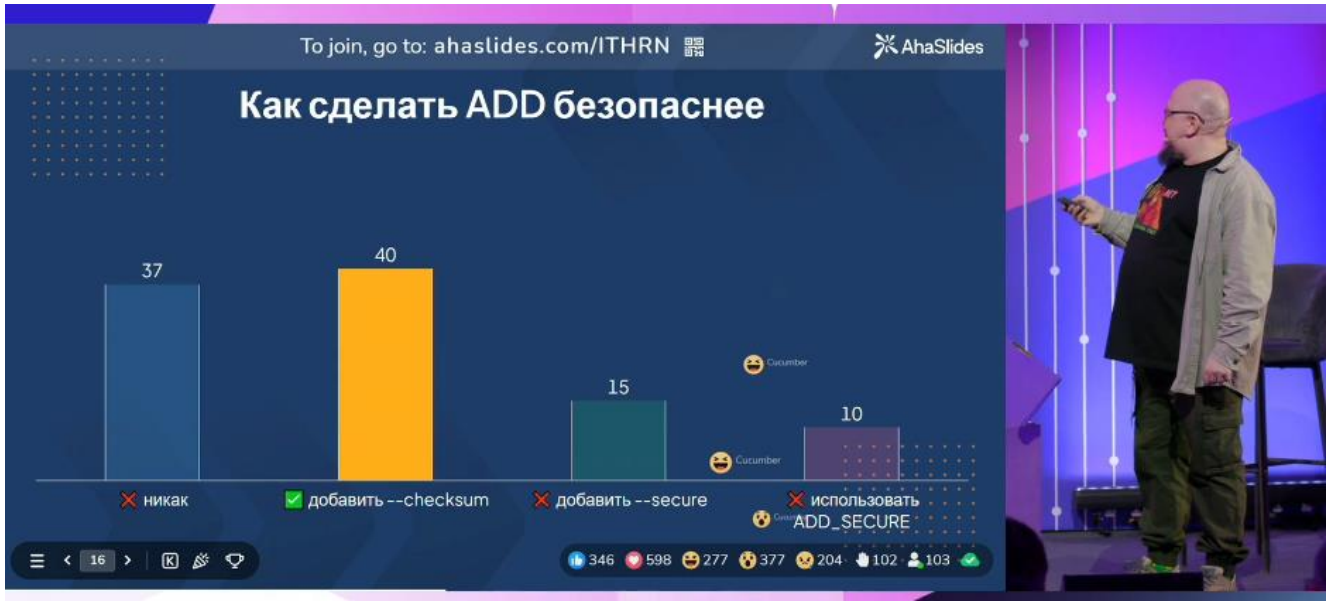
Мониторинг безопасности OSS

- Воронка уязвимостей: обновления, патчи, достижимые методы
- 83% уязвимости в транзитивных зависимостях

ссылка на доклад

Руководство Бравого Докер Секурити Мастера: latest

- Слайды квиза



доклад

Snatch: как стилеры помогают совершать целевые атаки

- Сценарий: долго незаметно пишут, потом сливают
- Доставка
  - Фишинг, GitHub, поддельные сайты, слитые программы
  - Малвертайзинг - рекомендации стилера вместо Zoom, ссылки на YouTube
  - ClickFix - инструкция от капчи: нажмите Win, CtrlV, Enter,....
- Выявление
  - Мониторить слитные учётки
  - Трафик от стилеров похож на нормальный
  - Способ выявления – тайпсквоттинг.
    - **PoC есть в ИЦ**, добавим?
- Как защищаться?
  - Смотреть, что запускаешь
  - Разрывать сессии (Google, например, долго хранит)

[доклад]

Со стенда PT NAD (офлайн)

- Метаданные
  - Хранят на SSD в Elastic 5.1, по сравнению с 5 уже сжали в 3 раза.
  - Планируют к концу года S3, ожидают сжатие ещё (?) в 8 раз.
- Трафик
  - Хранят в PCAPах без сжатия на HDD, менять не планируют.
  - Каждая сессия в отдельном PCAP, большие пилят на части по гигабайту.

Ещё интересные доклады

доклад
- Токены доступа и API gateway: как обеспечить безопасность запросов
  - opaque / self-contained токены
  - Точки инспекции, риски (безопасность / задержка)

доклад
- Легитимные C2: как популярные сервисы работают на хакеров
  - Telegram, WA, Discord для передачи отстуков
  - Детекция – по периодичности, иногда по содержимому, по контексту
    - трафик Discord без установленного приложения – но FP
    - Запросы к YouTube без браузерного приложения, частые обращения к API субтитров

доклад
- От яхтинга до рутинга: эксплуатация уязвимостей IoT для полной компрометации устройств
  - Реальная ситуация на моторных судах, устройство, возможности

доклад
- SDRcraft: искусство радиоэлектронной борьбы
  - Актуальные устройства для анализа радиосигнала

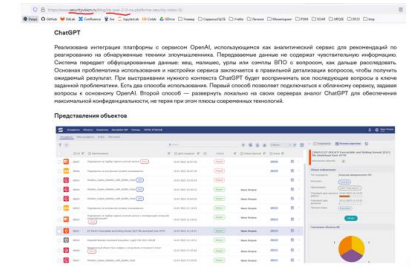
доклад
- Предсказуемывай это! Анализируем интернет быстро, качественно, дешево
  - Адаптивный скан, оптимизация сканирований (уход от прямоугольников в Masscan)

доклад
- Сколько стоит SOC на open source
  - Идеи хранилок

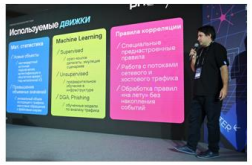
доклад
- Асинхронность vs. потоки: кто выживет в эпоху NoGIL?
  - Асинхронность даёт экономию ресурсов. Поток - 4МБ. Сокет - 4КБ. И при параллелизме на 10 тысяч потоков уже не хватает. И планировщик задач чуть тратит время на выбор
  - NoGIL: многопоточный код стал быстрее, а однопоточный - медленнее
  - В Python с GIL на 1 поток тратится 1 поток ОС, в Python nogil тоже можно использовать виртуальные потоки.

- Слайд из презентации про PHD 2024:

ML, AI, LLM, ChatGPT (?)… Правила!



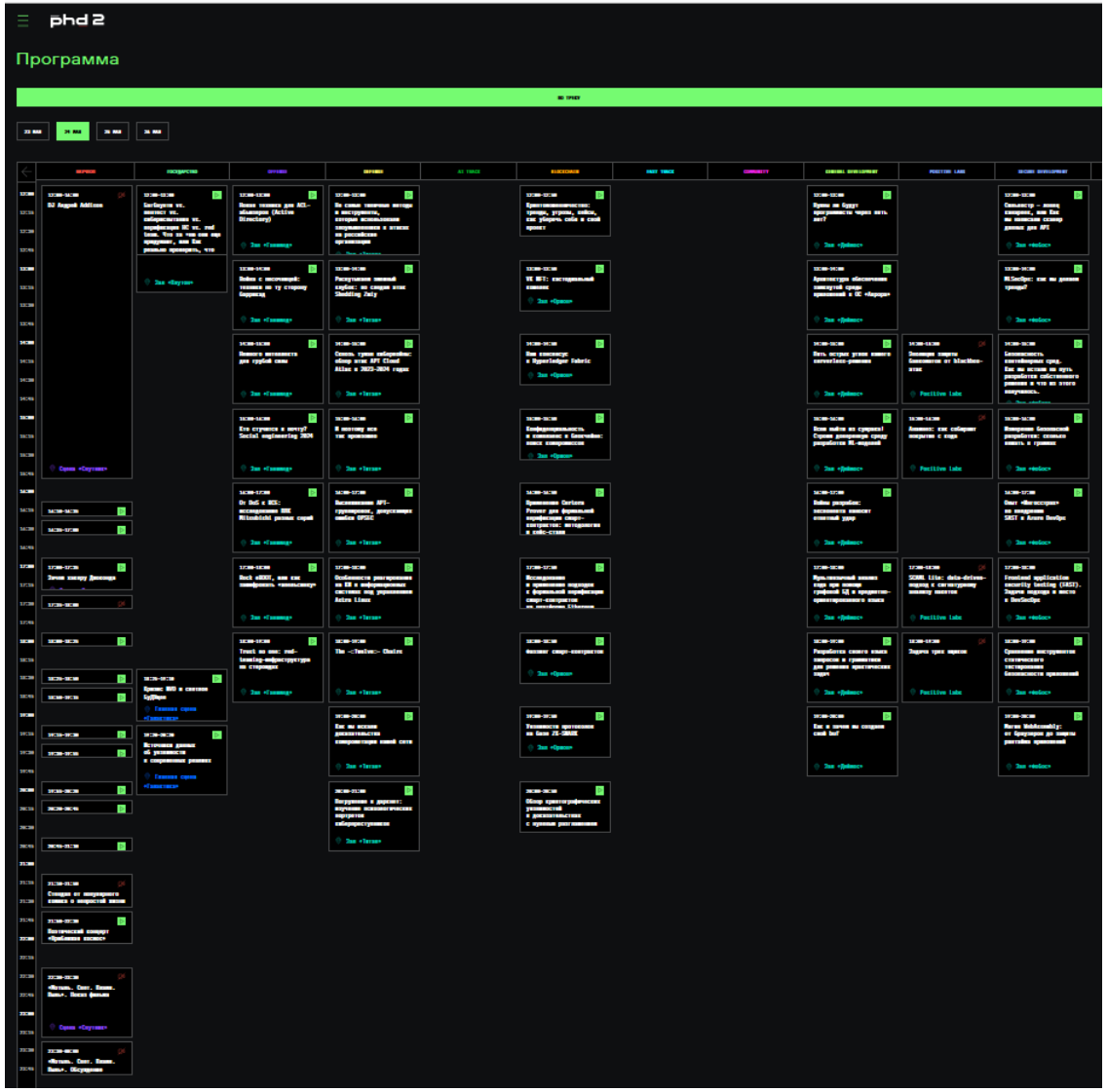
https://www.securityvision.ru/blog/irp-soar-2-0-na-platforme-security-vision-5/

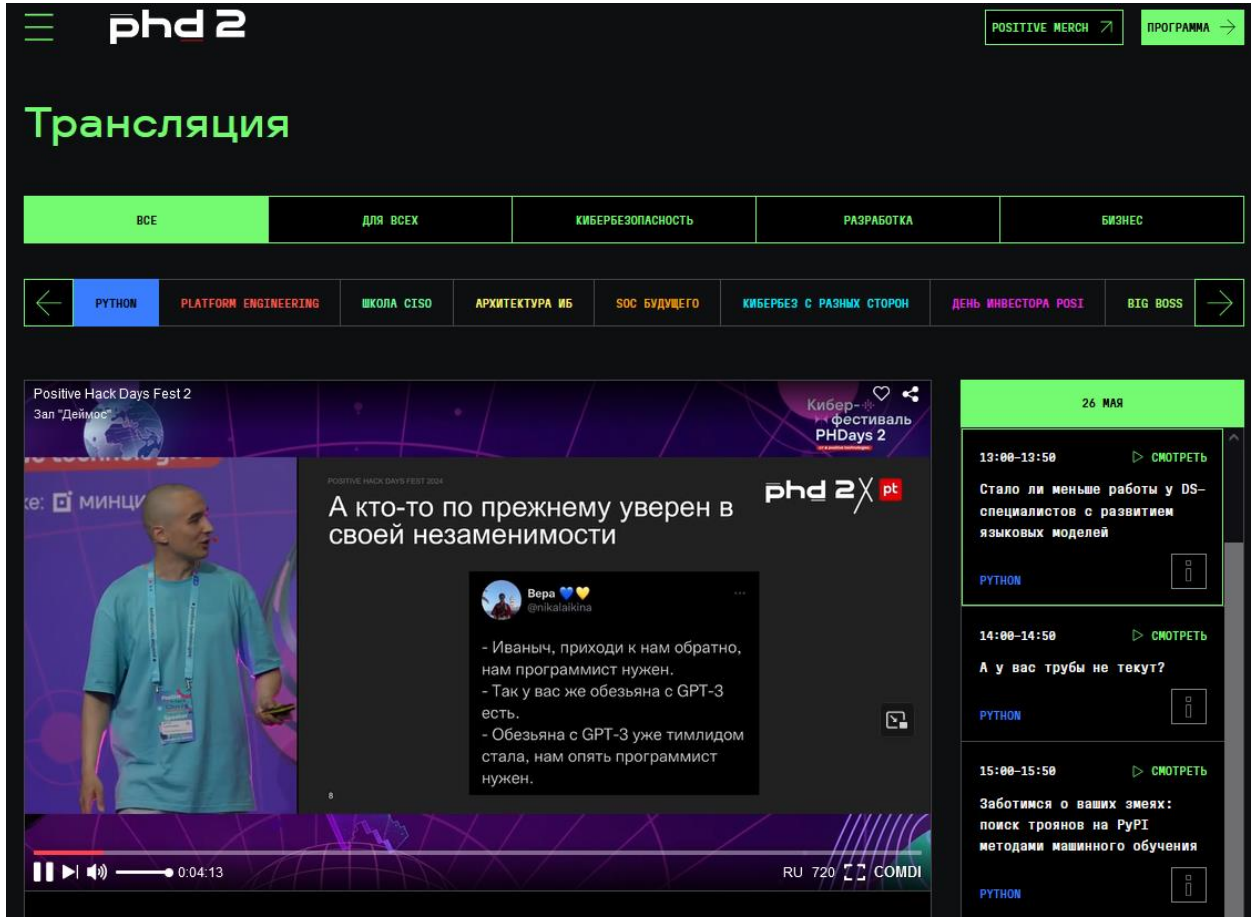


https://www.securityvision.ru/news/security-vision-na-phdays-13-kak-eto-bylo/

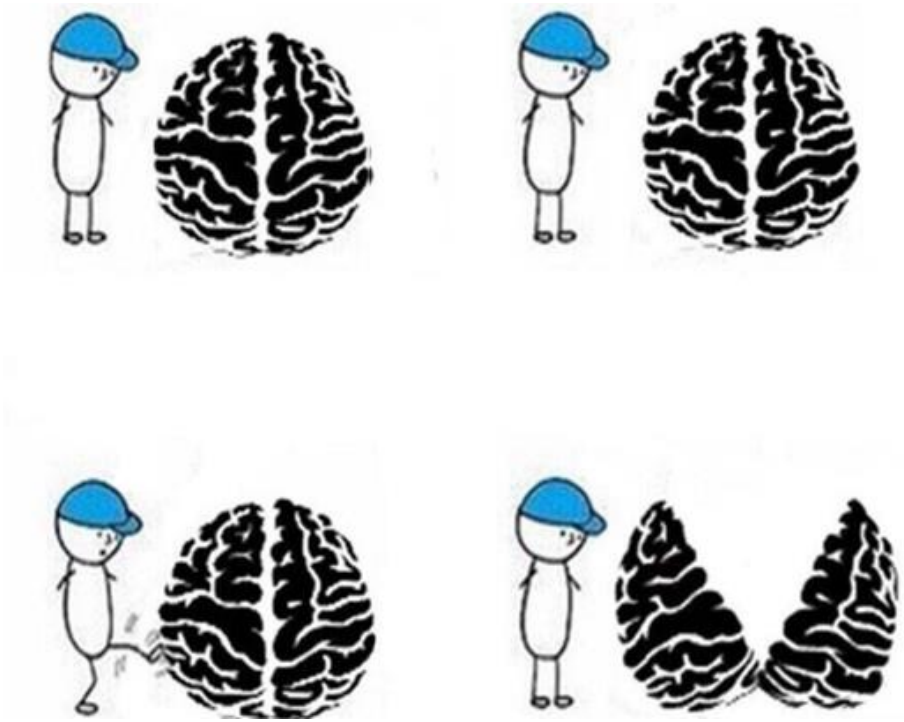
- Идея из 2025: большие модели шагнули вперёд, кто не использует сейчас – может не догнать потом

Послушать ещё? https://phdays.com/





Вне конфы



Полезные контакты

- Дмитрий Левшун – к.т.н. в ИТМО, занимается ML в ИБ (с И.В. Котенко)
- Абдулхамид Бучаев – аспирант ИТМО, диссер про анализ событий ИБ
- Михаил Васильев (Гарда, делает DCAP) – занимается аномалиями (https://onixlas.github.io/), решает задачи, применимые в NTA