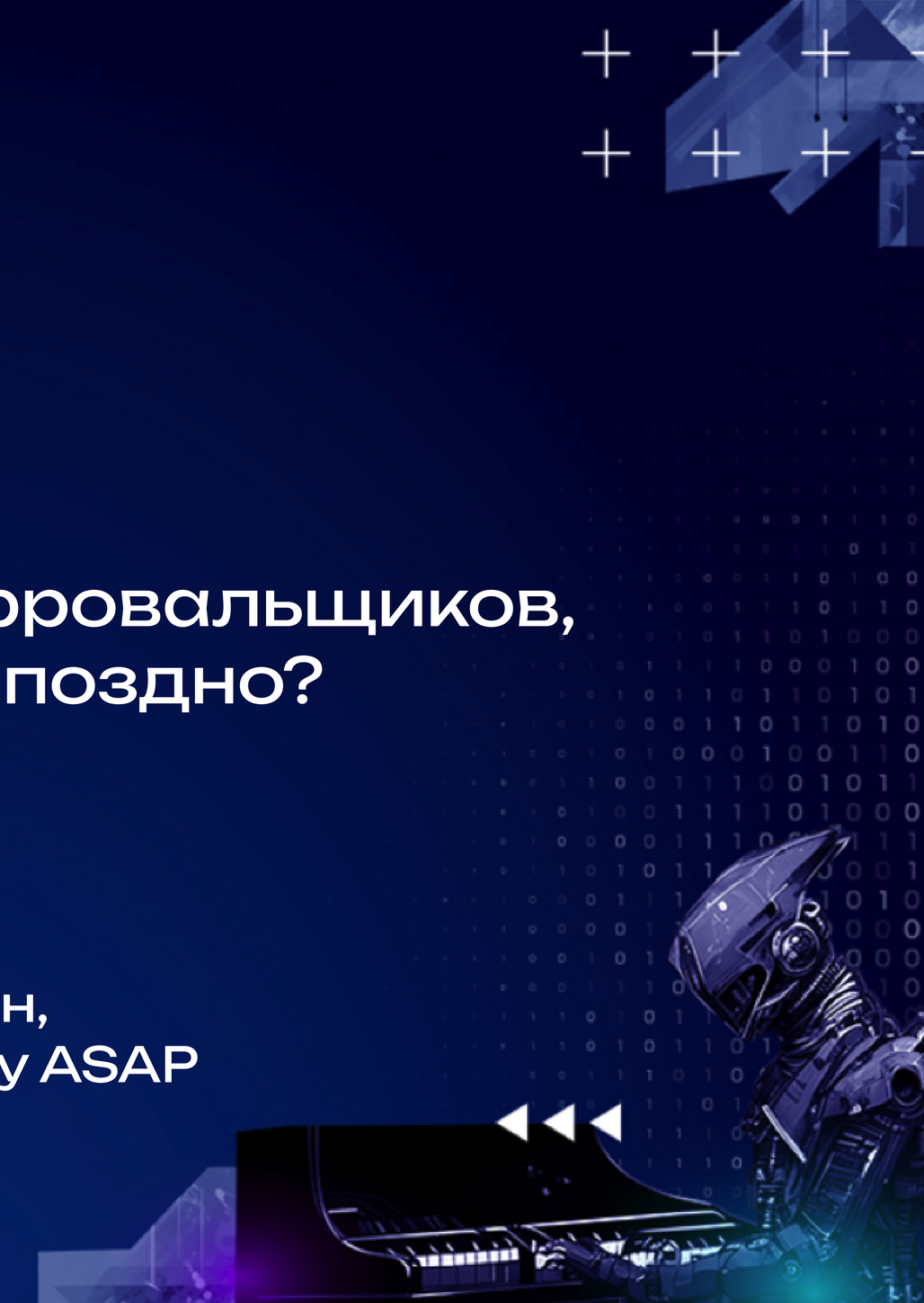
GIS DAYS

Обнаружение атаки шифровальщиков, как и когда еще не поздно?

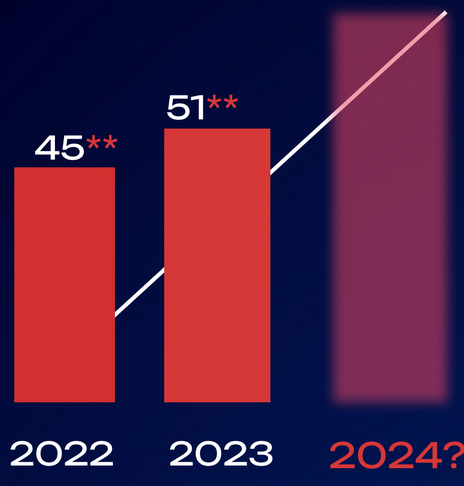
Виткова Л.А., ктн,
Product owner Ankey ASAP

2023

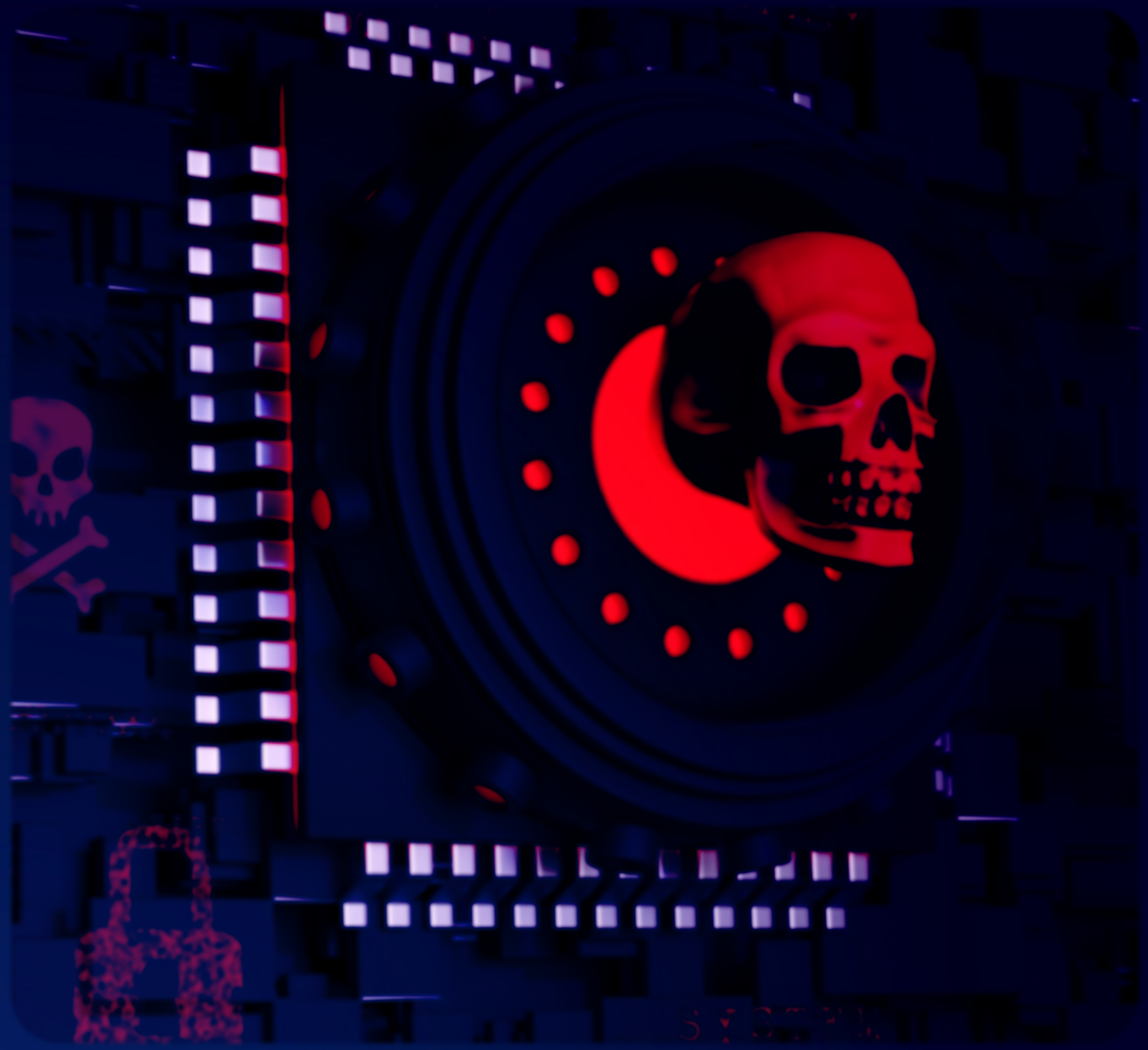


Шифровальщики — киберугроза №1

Почти четверть атак в 2023 году была связана с программами-вымогателями.*

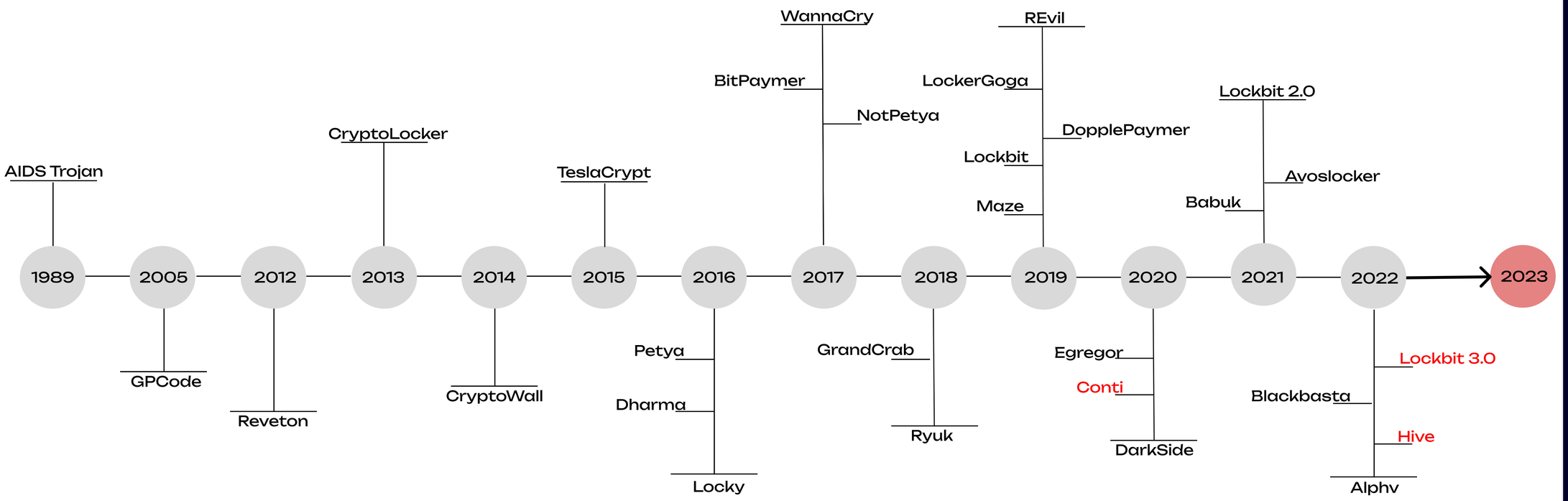


** Миллиарды рублей теряют организации, атакованные шифровальщиками



* IBM Security “Cost of a Data Breach Report 2023”

История программ вымогателей*

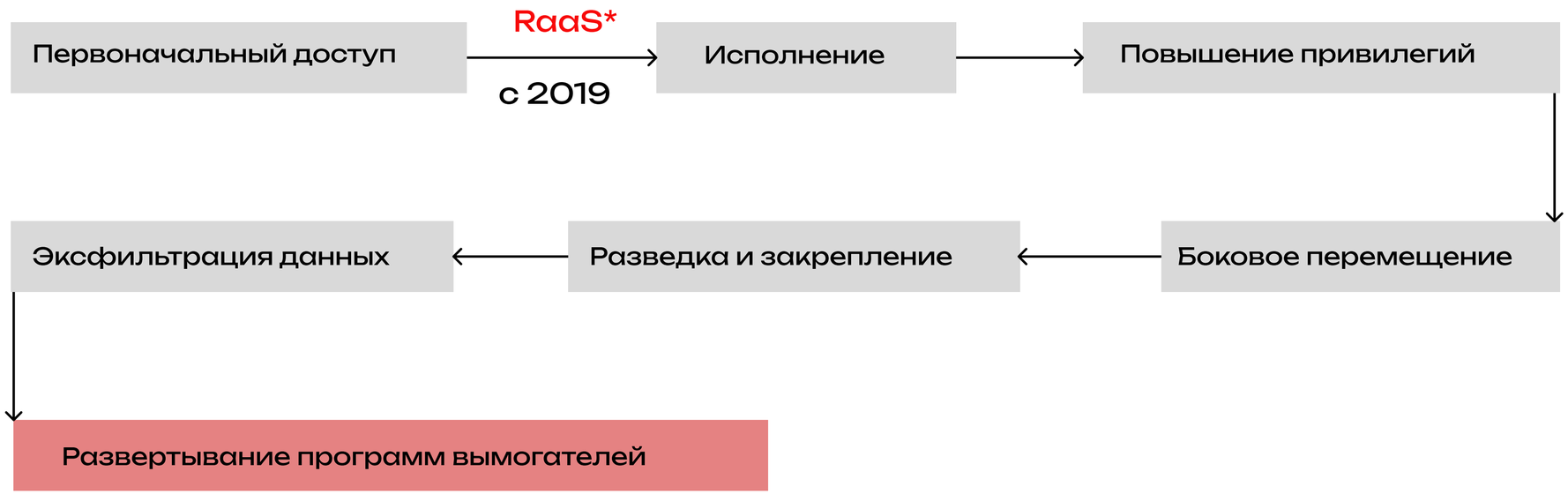


Красным выделены самые популярные шифровальщики для 2022 года**

*Warikoo A. Perspective Chapter: Ransomware. – 2023.
Submitted: September 21st, 2022 Reviewed: October 4th, 2022 Published: January 24th, 2023 DOI: 10.5772/intechopen.108433

** Опасная эволюция: Group-IB предупредила о главных киберугрозах 2023 года // F.A.C.C.T. Рейтинг на Хабр URL: https://habr.com/ru/companies/f_a_c_c_t/news/711068/

Жизненный цикл шифровальщика



По данным Trend Micro™ количество группировок RaaS только в 1 квартале 2023 года увеличилось на 12% С 39 шт в IV квартале 2022 до 45 шт в I квартале 2023

Количество атак с целью выкупа за расшифровку данных на бизнес в России в 2022 году увеличилось в три раза (F.A.C.C.T)

*Модель RaaS - вымогатель как услуга.

Ankey ASAP vs Шифровальщики

Вызов принят!

Большинство готовых наборов данных
не соответствуют корпоративным системам в России

Необходимы наборы и для ОС Windows и для Linux

Для оценки качества работы модели необходимы наборы со схожей активностью: архивация, запуск и установка программ, создание и перемещение файлов и тд.

Для оценки качества работы модели необходимы
смешанные наборы с нормальной и вредоносной активностью

Много публикаций в научных журналах с описанием идей по реализации подходов к обнаружению, но без детального описания экспериментов

Анализ этапов обнаружения (ч. 1)

ДОСТАВКА

MITRE: (IA) TA0001: T1133, T1190, T1566, T1204.002, T1195; (E) TA0002: T1204, T1059, T1203, T1047, T1053

ЖИЗНЕНЫЙ ЦИКЛ: первоначальный доступ

ВЕКТОРЫ: спам/фишинговая рассылка, целевой фишинг, веб-сервера, блокировка серверных сообщений, макросы, бэкдоры, известные уязвимости и уязвимости нулевого дня

ОБНАРУЖЕНИЕ: фишинг, социальный инжиниринг, инсайдеры, компрометация, запуск нелегетимных процессов, новое редкое действие

1

РАЗВЕРТЫВАНИЕ

MITRE: (P) TA0003: T1078, T1547, T1053, T1574, T1136, T1505; (DE) TA0005: T1218, T1222, T1055

ЖИЗНЕНЫЙ ЦИКЛ: исполнение, повышение привилегий, боковое перемещение, разведка и закрепление

ВЕКТОРЫ: загрузка библиотек и инструментов для дальнейших действий

ОБНАРУЖЕНИЕ: повышение привелегий, запуск не легетимных процессов, запуск терминальных команд, новое редкое действие, разведка

2

Анализ этапов обнаружения (ч. 2)

УНИЧТОЖЕНИЕ

MITRE: (D) TA0007: T1083, T1135
(C2) TA0011: T1071.001, T1001, T1105, T1573, T1102;
(I) TA0040: T1490, T1489, T1485, T1486, T1561

ЖИЗНЕНЫЙ ЦИКЛ: эксфильтрация данных, развертывание

ВЕКТОРЫ: обход каталогов и файлов, связь с контрольно-командным центром (C&C), процесс шифрования и/или удаления исходных файлов и теневых томов

ОБНАРУЖЕНИЕ: порождение деревьев процесса, корреляция между системными процессами, изменение типа файла, значительная модификация содержимого ...

3

УСТРАНЕНИЕ

MITRE: TA0010: T1041, T1567.002, T1020, TA0040

ЖИЗНЕНЫЙ ЦИКЛ: развертывание

ВЕКТОРЫ: пользователь, бизнес, собственник активов

ОБНАРУЖЕНИЕ: подходит под обнаружение стиллеров и/или на обнаружение артефактов DLS

4

Распространенные поведенческие признаки

Признак	Комментарий
Энтропия записи	Варианты: (1) общая энтропия файла; (2) средняя разница операций чтения и записи; (3) отдельные операции записи.
Перезапись файлов	Исходный файл полностью перезаписывается зашифрованными данными или случайными данными
Обход каталога	Процессы ransomware выполняют операции открытия для каждого файла в каталоге
Перечисление каталогов	Ransomware для поиска интересующих файлов выполняет большое количество операций по перечислению файлов
Межфайловый доступ	Ransomware получает доступ к разным типам файлов, в то время как легитимные процессы к определенному подмножеству.
Операции: чтения/ записи/ открытия/ создания/ закрытия	Для ransomware свойственно зашифровать как можно больше файлов в каталогах жертвы. Основной индикатор в существующих поведенческих детекторах
Временные файлы	Некоторые семейства программ-вымогателей используют временные файлы в качестве буфера для шифрования файлов
Покрытие типов файлов	Есть семейства ransomware шифрующие все данные в том числе и exe. Легитимные программы обычно получают доступ только к части файлов.
Сходство файлов	Общее сходство файлов до и после операций записи от данного процесса.
Изменение типа файла	Шифрование файла влечет за собой изменение магических байтов, эффективно изменяя сигнатуру типа файла.
Частота доступа	Ransomware стремится зашифровать пользовательские файлы как можно быстрее.

Уклонение от поведенческих классификаторов

1.1 Традиционная атака ransomware

– соответствует типичным распространенным семействам ransomware.

1.2. Атака уклоняющегося ransomware

– соответствует сложным программам,

имитирует поведение легитимных процессов.

1.3 Адаптивная атака ransomware

– соответствует сложной уклоняющейся атаке,

направленной на снижение выраженности файловых функций.

Локальная видимость

Разделение процессов

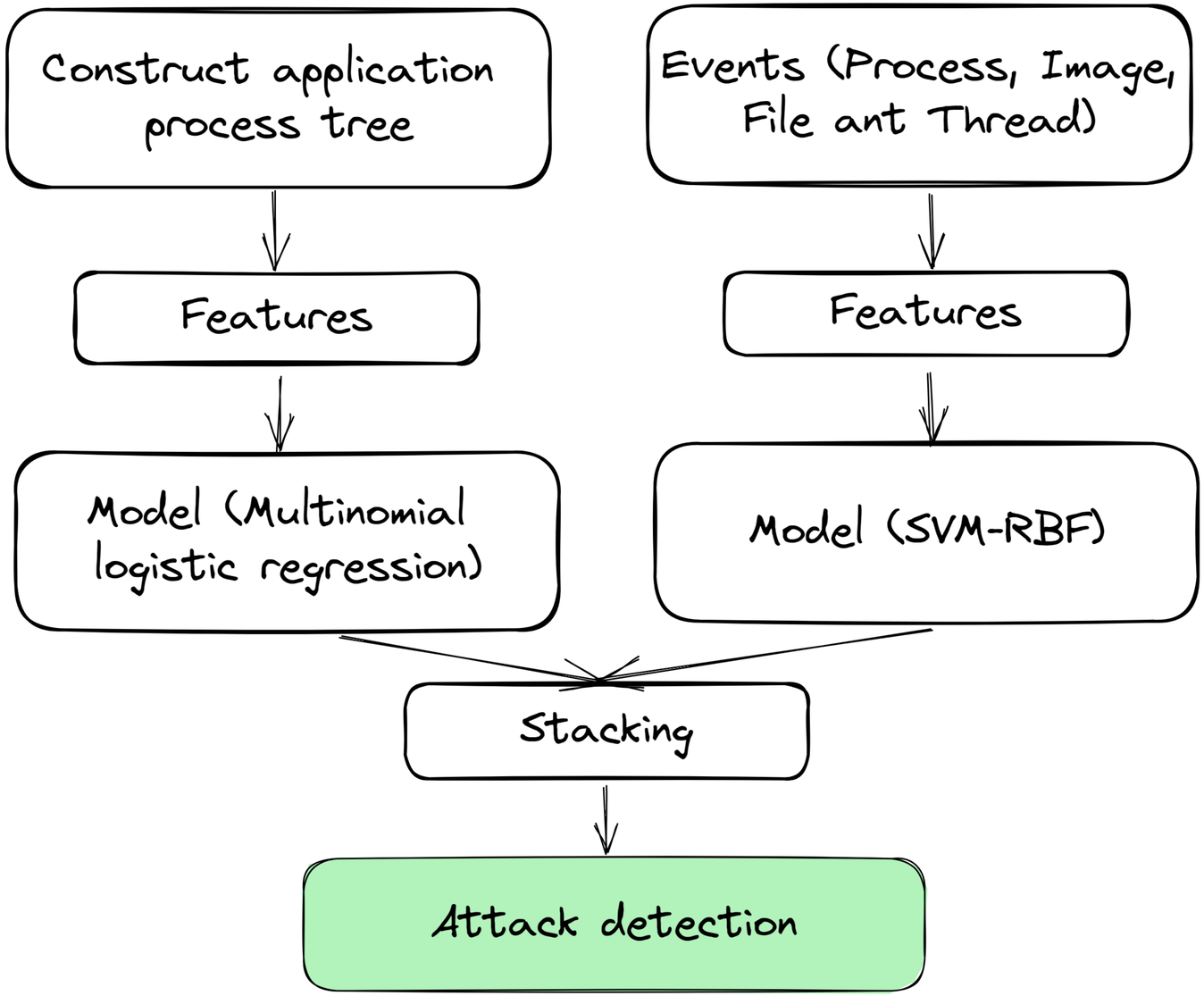
Сокрытие операций записи

Негибкость детектора

Мимикрия

Функциональное разделение

Подход 1. Создание профиля поведения (event OC)

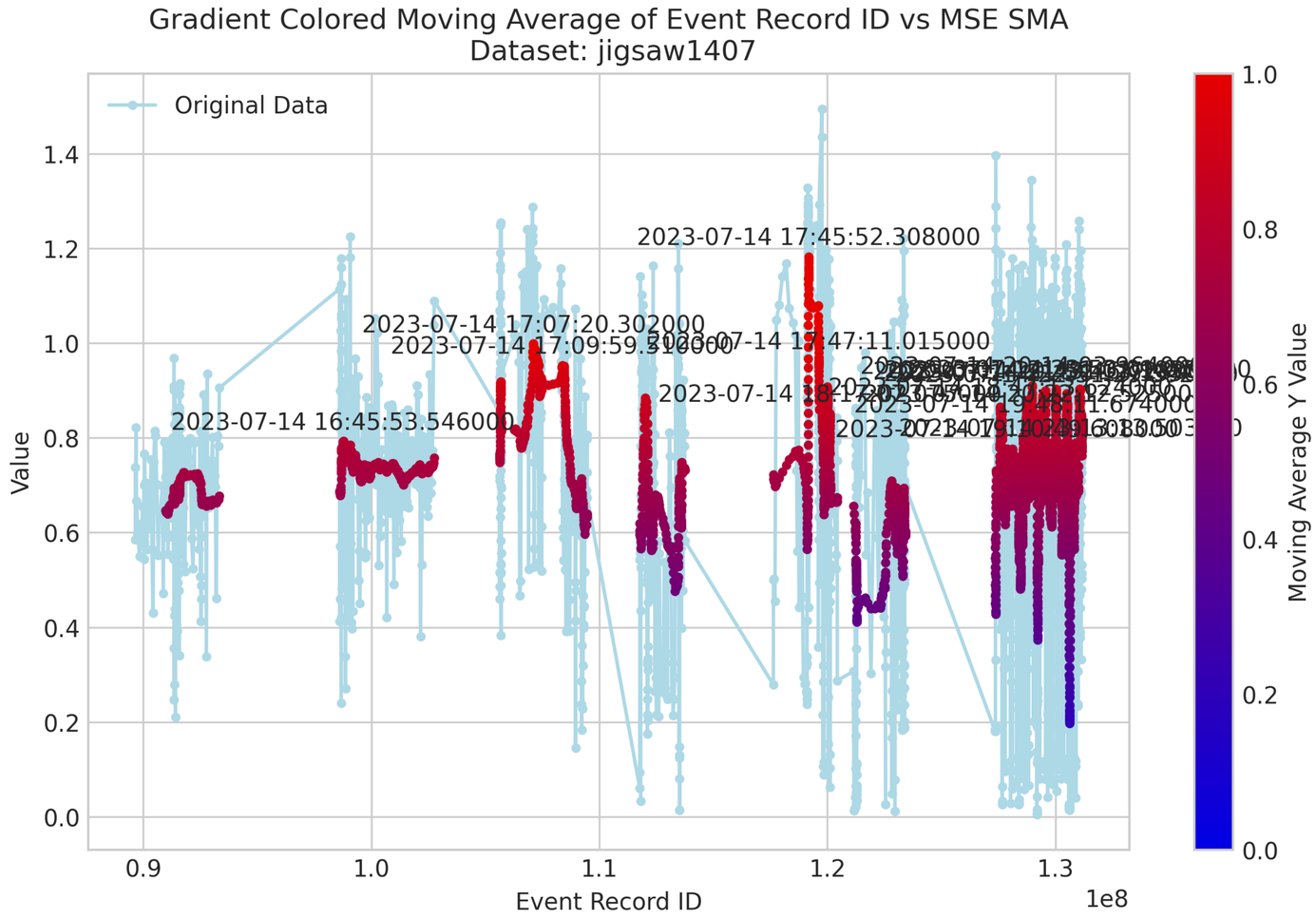


Модель логистической регрессии работает с признаками, полученными из дерева процессов

Модель SVM работает с количественными признаками операций процессов

Далее используется объединение двух моделей (Stacking-алгоритм ансамблирования)

Подход 2. Искусственная нейронная сеть LSTM



Пример обнаружения шифровальщика jigsaw со смешанной нормальной активностью

Обучается нейросеть на нормальной активности хоста (пользователя)

Подход применим для разных типов угроз (разведка, активность ботнетов и тд.)

Подход применим для обнаружения 0-day угроз

Обученная модель применима для федеративного обучения (вес модели 26 Мб)

Итак! Когда не поздно?

В тот момент, когда шифровальщик начинает работать на хосте - еще не поздно, можно заблокировать процесс, можно заблокировать хост. Можно спасти и инфраструктуру, и данные, и деньги, пожертвовав малым

Перенос обученной модели на хост (EDR решения) позволит в краткие сроки обнаружить атаку шифровальщика

Для обнаружения шифровальщика необходимо внедрять ИИ. Это позволит быстро проанализировать большие потоки данных. Базовая аналитика построенная на логике - не справляется. От сигнатурных методов шифровальщики уклоняются

GIS DAYS

Спасибо за внимание!

Виткова Л.А., ктн,
Product owner Ankey ASAP