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

Светлана Старовойт

21 09 2023 МОСКВА

ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ

ТЕХНО infotecs ФЕСТ

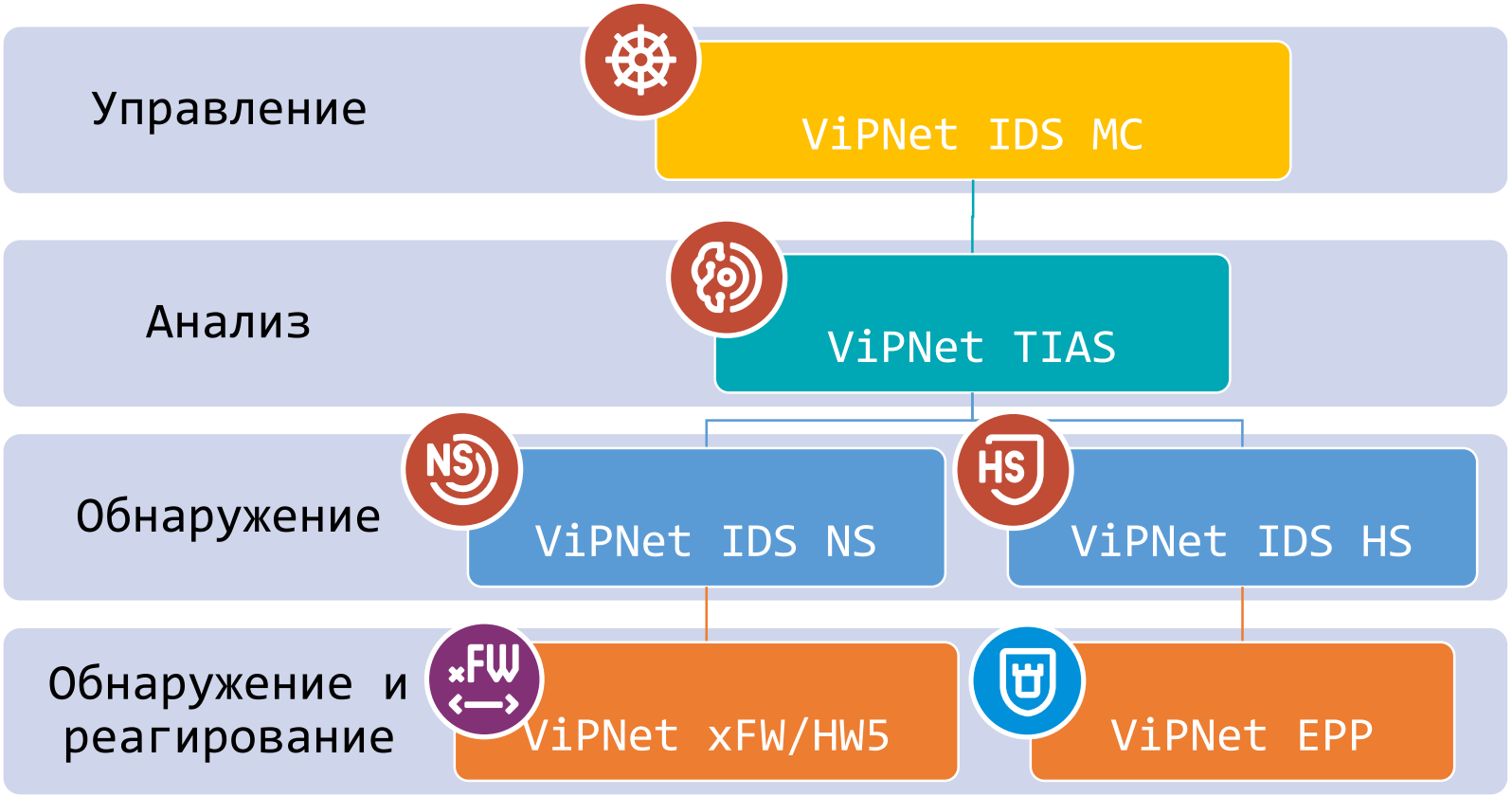
ТЕХНО infotecs 2023 ФЕСТ

Напомню о некоторых важных и полезных функциях в продукте

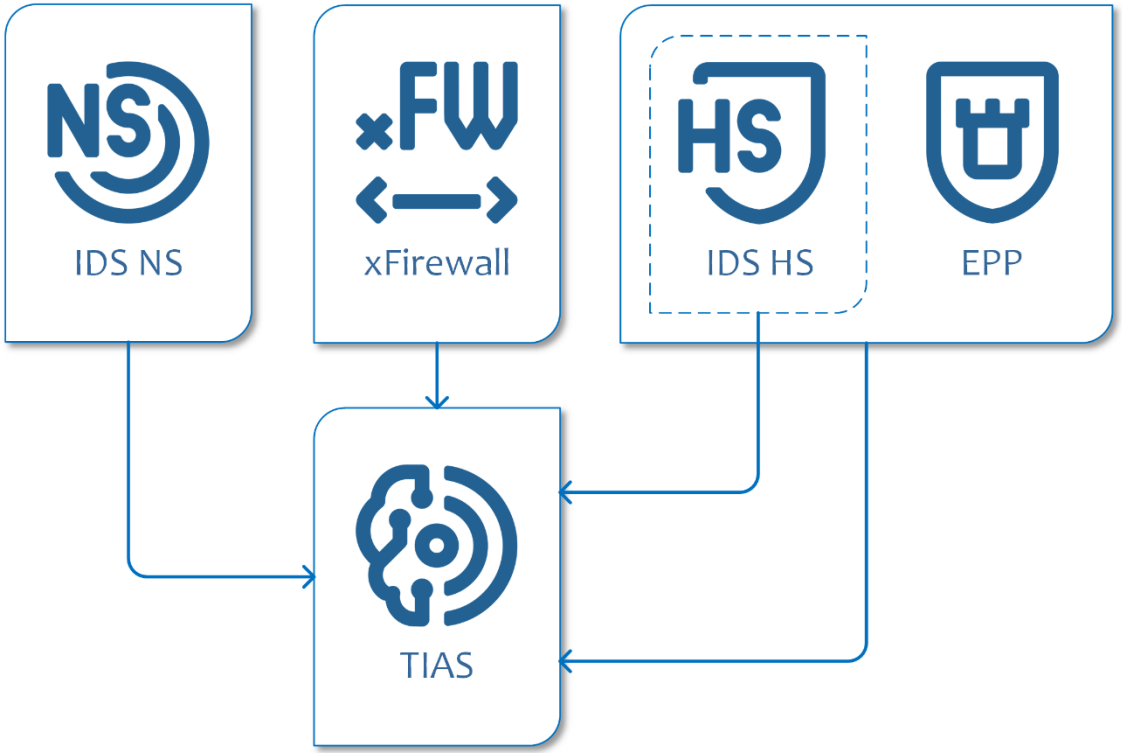
Расскажу об основных изменениях в новой версии

Покажу новые сценарии работы

Решение ViPNet TDR



Источники событий ViPNet TIAS



ViPNet TIAS 3.8

Основные улучшения и новые возможности

Пользовательские метаправила
возможность написания собственных правил анализа событий и выявления инцидентов

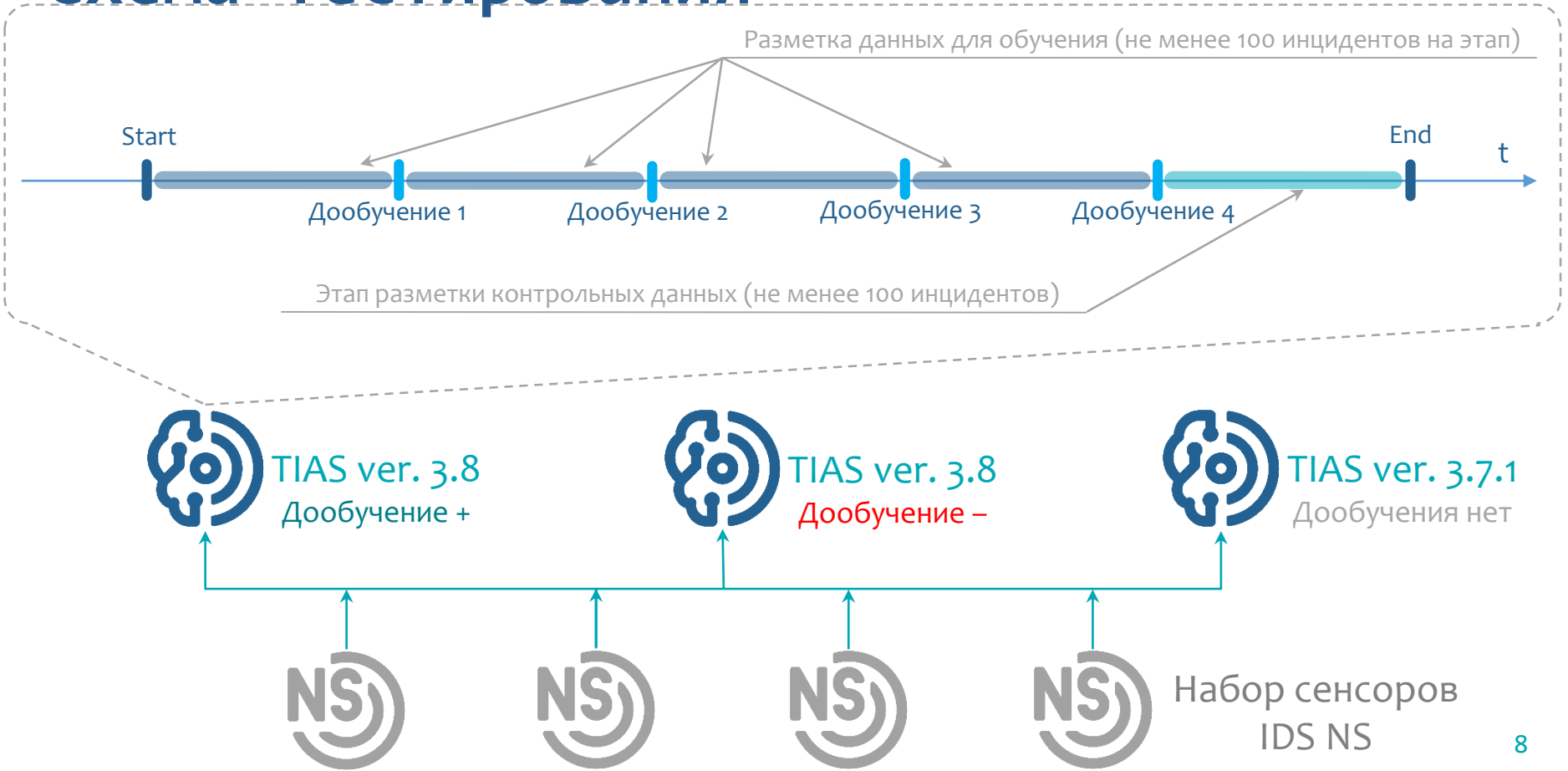
Дообучение модели
возможность дообучения модели машинного обучения как на новых экспертных данных, так и на размеченных данных пользователей

Новый источник событий
Прием и обработка событий ИБ, от шлюза безопасности ViPNet Coordinator HW 5

Демо. Пользовательские метаправила

Дообучение модели

Схема тестирования



Результаты

Инциденты на TIAS 3.8 с дообучением	Процент подтвержденных среди размеченных	Всего инцидентов в будни	Среднее количество инцидентов в будний день
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 %).

infotecs

Мастер-класс.
Переходим к практике!

ТЕХНО 2023 infotecs ФЕСТ

Спасибо за внимание!

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363