Искусственный интеллект на страже безопасности.

Обнаружение компьютерной атаки моделями машинного обучения решения ViPNet TDR

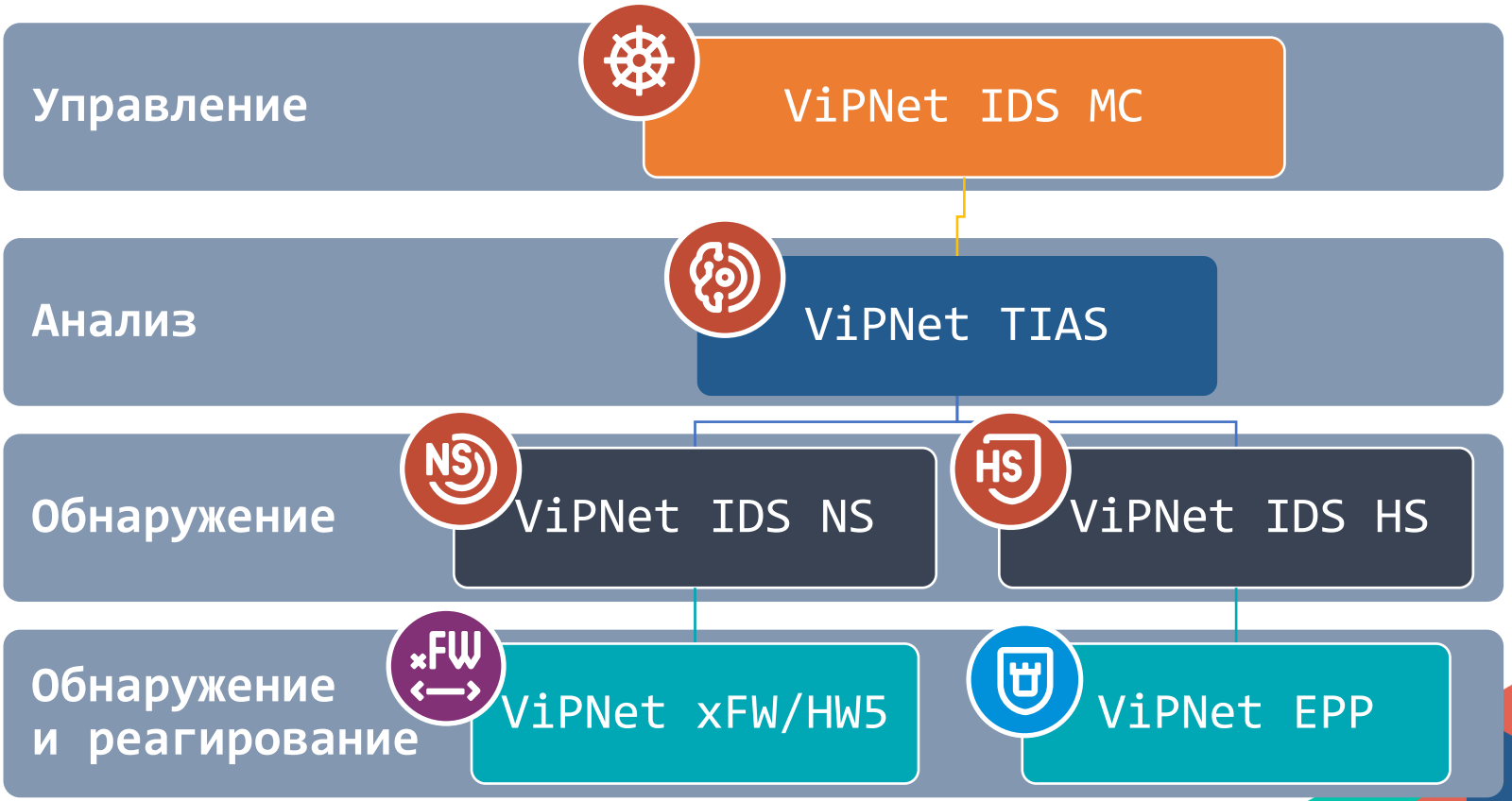
Светлана Старовойт

Руководитель продуктового направления

инфотекс ТЕХНОДЕСТ

Красный поток

Решение ViPNet TDR



Версии продуктов, которые показываем

- ViPNet IDS NS 3.11
- ViPNet IDS MC 1.11
- ViPNet TIAS 3.11

Новые сценарии в NS

Построение графа взаимодействия

Просмотр содержимого PCAP-файлов

Отображение информации об узлах на графе потоков

ML-модели в ViPNet IDS NS и ViPNet TIAS

Обнаружение сгенерированных доменных имен

DGA

Обнаружение фишинговых доменных имен

FDA

Обнаружения вредоносного ПО в TLS-трафике

JA3

Обнаружение вредоносной активности в событиях в TIAS

SID-Chain

Новые сценарии в ViPNet TIAS

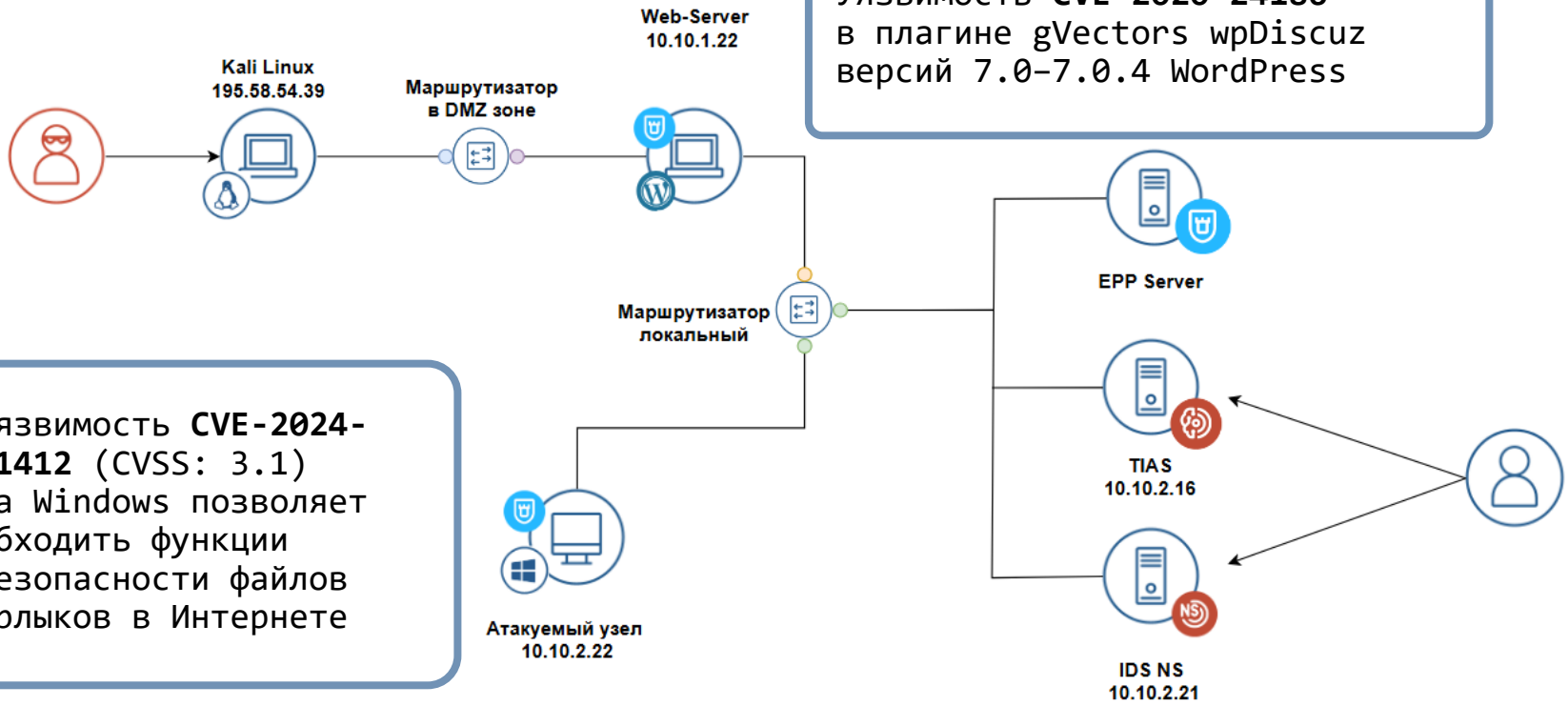
Горизонтальное распространение инцидентов

Связывание инцидентов

Новые метаправила для ML-событий

Схема стенда

Уязвимость **CVE-2020-24186** в плагине gVectors wpDiscuz версий 7.0–7.0.4 WordPress



Уязвимость **CVE-2024-21412** (CVSS: 3.1) на Windows позволяет обходить функции безопасности файлов ярлыков в Интернете

Описание атаки

Шаг 1. Фишинг на Windows (CVE-2024-21412)

TA0001 Первоначальный доступ

T1566.002 Целевой фишинг со ссылкой

Шаг 3. Сканирование сети в DMZ зоне

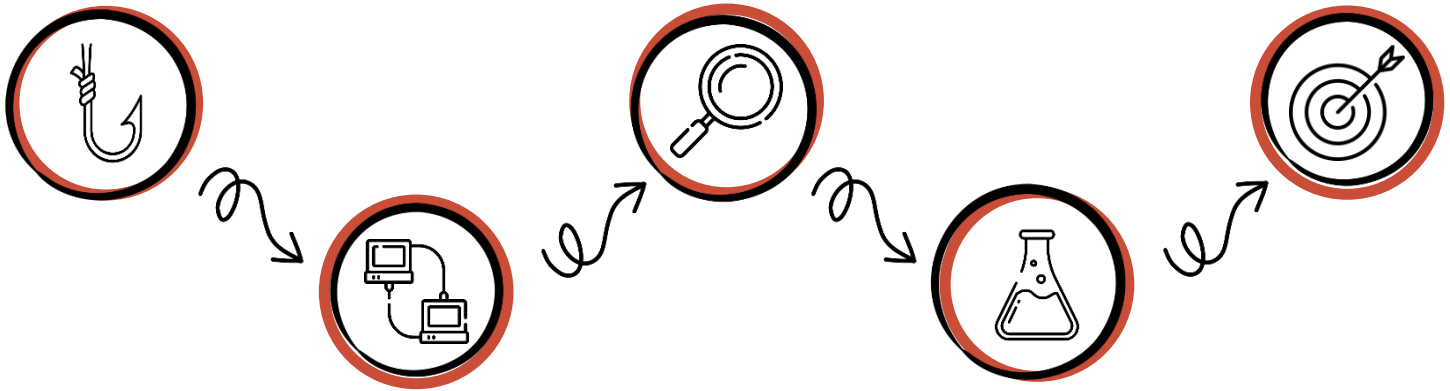
TA0007 Обнаружение

T1046 Изучение сетевых служб

Шаг 5. Кража данных

TA0010 Эксфильтрация данных

T1041 Эксфильтрация по каналу управления



Шаг 2. Установление meterpreter-сессии с Windows

TA0011 Организация управления

T1071 Протокол прикладного уровня

Шаг 4. Эксплуатация уязвимости CVE-2020-24186 Wordpress с плагином wpDiscuz

TA0001 Первоначальный доступ

T1190 Эксплуатация уязвимостей публичных приложений

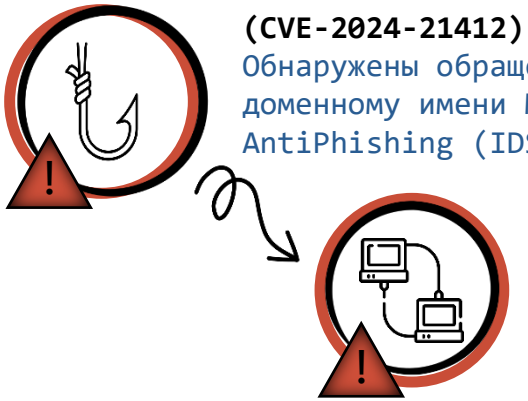
ВНИМАНИЕ!

Компьютерная атака воспроизводится в демонстрационных целях.

Мы не призываем и не обучаем вас атаковать компьютерные системы.

И помните: киберпреступления караются законом.

Отслеживание последовательной атаки компонентами TDR



Шаг 1. Фишинг на Windows (CVE-2024-21412)

Обнаружены обращения к фишинговому доменному имени ML-моделью AntiPhishing (IDS NS)

Регистрация сигнатурных инцидентов в TIAS

Эксплуатация уязвимости CVE-2024-21412 (тип метаправила «Последовательность событий»)

Обращение к фишинговому доменному имени (тип метаправила «ML-событие»)

Шаг 2. Установление meterpreter-сессии с Windows

Обнаружено обращение к сгенерированным доменным именам ML-моделью DGA (IDS NS)

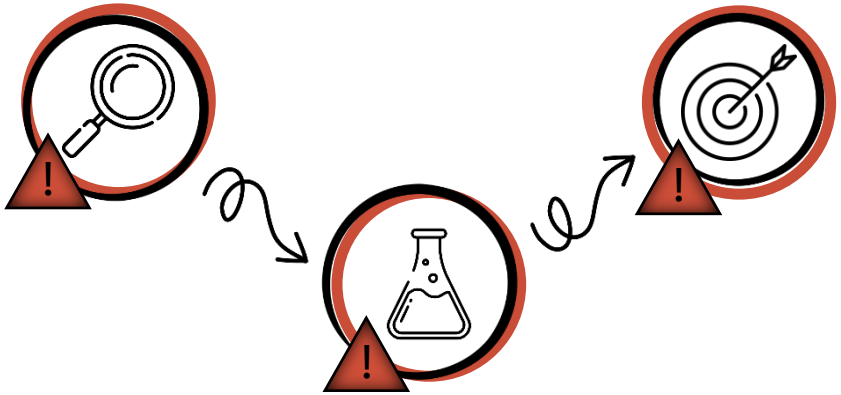
Обнаружена нежелательная программа в зашифрованном трафике методом Malware JA3 (IDS NS)

Отслеживание последовательной атаки компонентами TDR

Шаг 3. Сканирование сети в DMZ зоне

Шаг 5. Кража данных

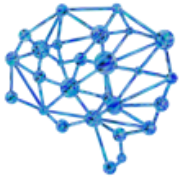
Обнаружено аномальное увеличение исходящего трафика ML-моделью TVA



Шаг 4. Эксплуатация уязвимости CVE-2020-24186 Wordpress с плагином wpDiscuz

Регистрация сигнатурных событий в IDS NS и ViPNet EPP

Регистрация эвристического инцидента в TIAS



Классификатором обнаружена подозрительная активность (модель SID-Chain)

САНКТ ПЕТЕРБУРГ

инфотекс

ТЕХНОФЕСТ

Подписывайтесь на наши соцсети

инфотекс Академия · Учебный центр инфотекс · AMPIRE · TELEOFIS · КОМФОРТЕЛ оператор связи бизнес-класса · РУТОКЕН компания ПРАКТИВ · TS Solution · AXOFT