Система для выявления аномалий сетевого трафика, основанная на машинном обучении

ПРОБЛЕМА

К анализу сетевого трафика неприменимы классические методы ИБ, рыночные решения для производства затратны

РЕШЕНИЕ

FoilHat - ELK Stack
“коробочная” платформа поиска сетевых аномалий

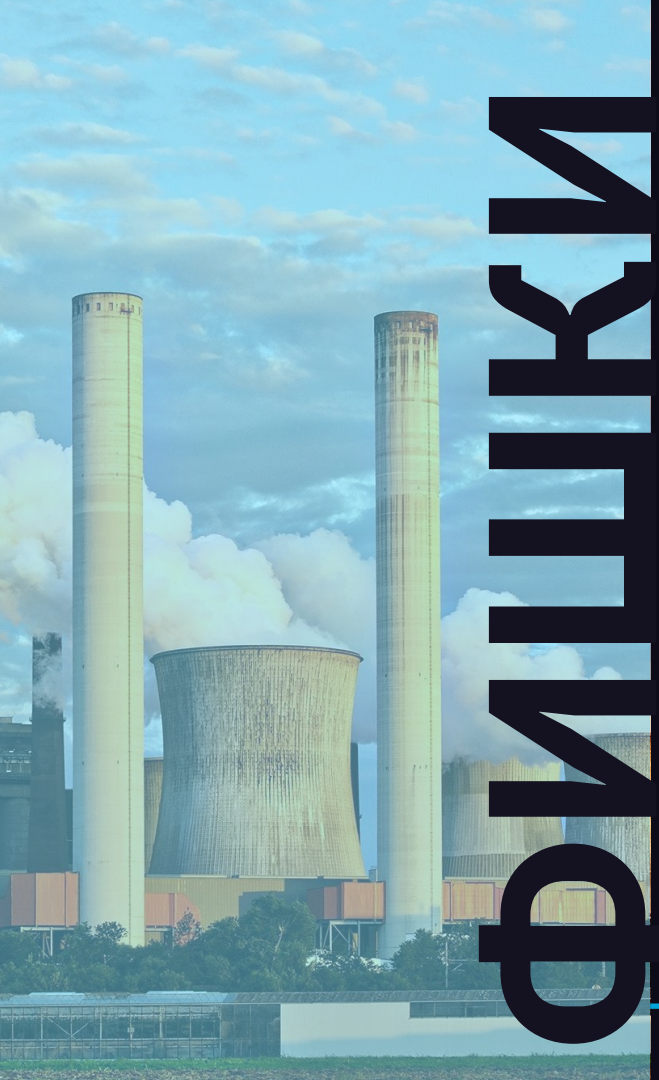
Инновационность заключается в

Поддержке 35 сетевых протоколов из “коробки”

Авто-уведомлениях об атаке с помощью СМС

Двойном машинном обучение Foilhat + Kibana

Веб-интерфейсе с сигналами об атаке и репортами для SOC



ФИШКИ

Мы ориентируемся на КИИ

Поддержка специфических протоколов КИИ

Реализация системы на GO с защитой от утечек памяти

Дешевое внедрение системы в производство

КИИ - критическая информационная инфраструктура

Ожидаемое качество работы **только FOILHAT**

11 мин
время обучения протокола

50 гб
трафика для нейросети

98%
точность нейросети

Осуществленные тесты на протоколе TCP

18 мин
время обучения протокола

25 гб
трафика для нейросети

99,12%
точность нейросети

Способы встраивания решения

При защите критических инфраструктур (ICS)

Интернет трафик

На hardware перехватываем трафик (mitm)

Видеокамеры

Рабочие места

Производственные устройства

При защите офисных сетей КИИ

Интернет трафик

решение

Офисная сеть

Обзор 4-ех основных конкурентов

	FoilHat	PacketBeats	Zeek NSM	Kaspersky OS	Suricata
Поддержка протоколов	< 35	13	50	кастомно	19
Цена решения	$1000/устр.	$200/мес	OpenSource	от $20000/устр.	OpenSource
Работа с КИИ (критическими инфраструктурами)	+	--	--	+	--
Корреляция данных	+	+	--	--	--
Безопасность памяти	+	+	--	+	--
Время внедрения	**2 недели**	--	--	**от 3 месяцев**	--

Zeek NSM, Suricata, PacketBeats - лишь фреймворки, осуществляющие анализ. Kaspersky OS - полноценное решение, основная проблема которого сложность внедрения (клиент должен сам разрабатывать по для ОС)

Показатели рынка

мы тут

ПО для SOC
$18 млрд. 2021

Реагирование на инциденты.
$35 млрд. в 2021

Вирусный анализ

Мировой рынок ИБ $200 млрд. в 2021

40%
Q4 2019 - Q1 2022

* Анализ отчета исследования рынка кибербезопасности KPMG

Ориентировочная **прибыль** Q4 2 года - $ 30 тыс/мес

Что мы продаем:

- Лицензию компаниям на использование ПО для hardware
- ПО для сетевой защиты (файервол) как для МСП так и для корпораций

Цена на лицензию:

- Цена на лицензию за защиту устройства $ 1.000 в месяц для бизнеса.
- Цена для вендоров оборудования - договорная.

Целевая Аудитория:
-> SOC/SIEM команды компаний

Задачи в рамках этапов

1. Разработка архитектуры фреймворка;
2. Разработка модуля сбора трафика инфраструктуры (и его расшифровки).
3. Разработка модуля обработки данных сетевых протоколов (PCAP);
4. Разработка драйверов для сбора трафика с hardware девайсов.

II ЭТАП

1. Разработка модуля машинного обучения (на основе TensorFlow) и разметки датасета;
2. Проведение обучения и тестирование системы (поиск наилучших значений для работы);
3. Разработка и настройка веб-интерфейса для работы аналитической панели;
4. Разработка модуля уведомления SOC/SIEM о найденных аномалиях, разработка модуля отчетности.
5. Тестирование системы с использованием реальных датасетов

Custdev Huawei показал спрос на решение

Денис Николаевич Макрушин
Руководитель группы перспективных исследований безопасности Huawei

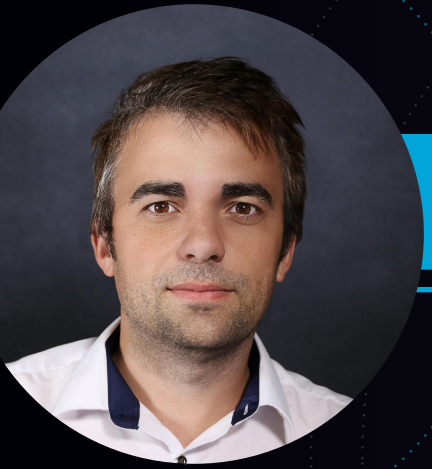
Мы провели custdev Huawei, потому что:

- Компания является крупнейшим производителем сетевого оборудования
- Активно развивает направление информационной безопасности

Компания проявила интерес, потому что технология может быть интегрирована:

- Коммутаторы huawei cloudengine
- Huawei G3 маршрутизаторы
- Series MID-RANGE Service routers

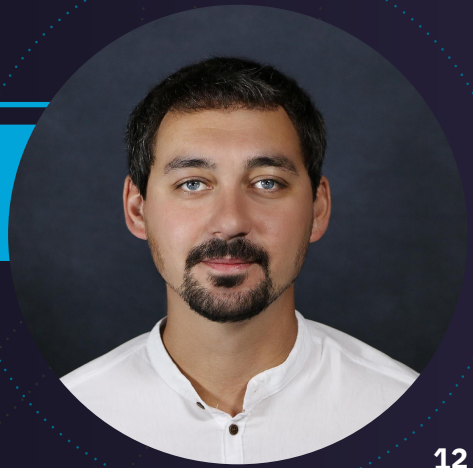
Команда проекта



Евгений Ларионов

35 лет, Генеральный директор

Идейный автор, занимается менеджментом, дизайном, бизнесом. Победитель Цифрового Прорыва. Имеет опыт в бизнесе 10 лет.



Виктор Горюнов

34 года, Программист

Системный администратор, победитель Цифрового прорыва. Разработчик: Python (TensorFlow), C/C++, PHP.

Поддерживаемые протоколы

+ TLS (Client Hello Msg + Ja3)
+ LinkFlow
+ NetworkFlow
+ TransportFlow
+ HTTP
+ Flow (unidirectional)
+ Connection (bidirectional)

+ NTP
+ SIP
+ IGMP
+ LLC
+ IPv6HopByHop
+ SCTP
+ SNAP
+ LinkLayerDiscovery
+ ICMPv6NeighborAdvertisement
+ ICMPv6RouterAdvertisement
+ EthernetCTP
+ EthernetCTPReply
+ LinkLayerDiscoveryInfo

+ TCP
+ UDP
+ IPv4
+ IPv6
+ DHCPv4
+ DHCPv6
+ ICMPv4
+ ICMPv6
+ ICMPv6Echo
+ ICMPv6NeighborSolicitation
+ ICMPv6RouterSolicitation
+ DNS
+ ARP
+ Ethernet + Dot1Q
+ Dot11