

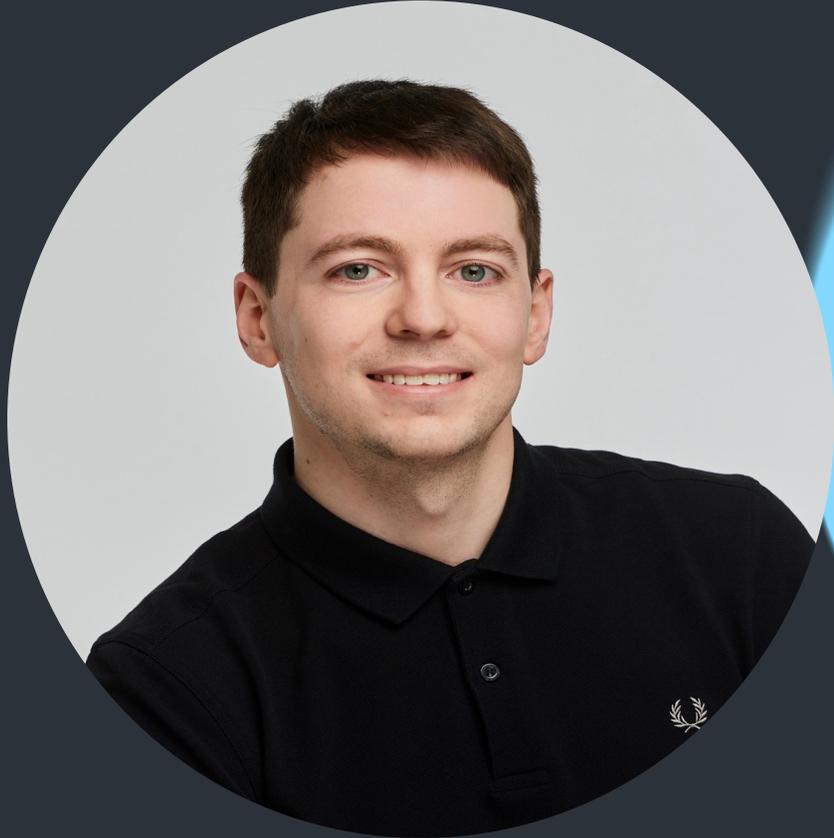
SOC
FORUM
2023

Варианты Open Source-ловушек, фреймворки по их управлению и мониторингу

Дмитрий Асташкин
Дмитрий Черников

Москва, 2023

SOC
FORUM
2023



Дмитрий Асташкин



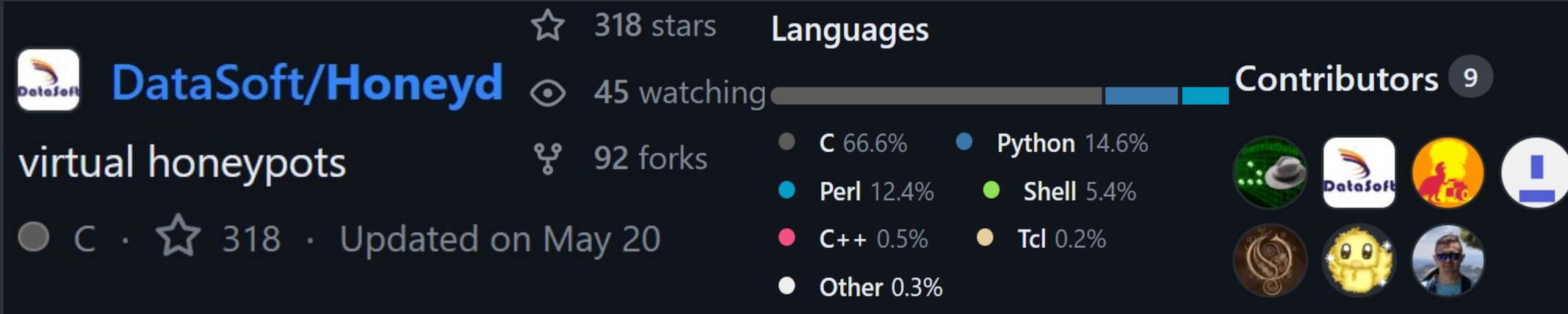
Дмитрий Черников

Сколько Open Source-проектов
ханипотов на GitHub?

4 0000+

Поговорим о honeypot

HONEYD



DataSoft/Honeyd virtual honeypots

318 stars · 45 watching · 92 forks · Updated on May 20

Languages

- C 66.6%
- Python 14.6%
- Perl 12.4%
- Shell 5.4%
- C++ 0.5%
- Tcl 0.2%
- Other 0.3%

Contributors 9

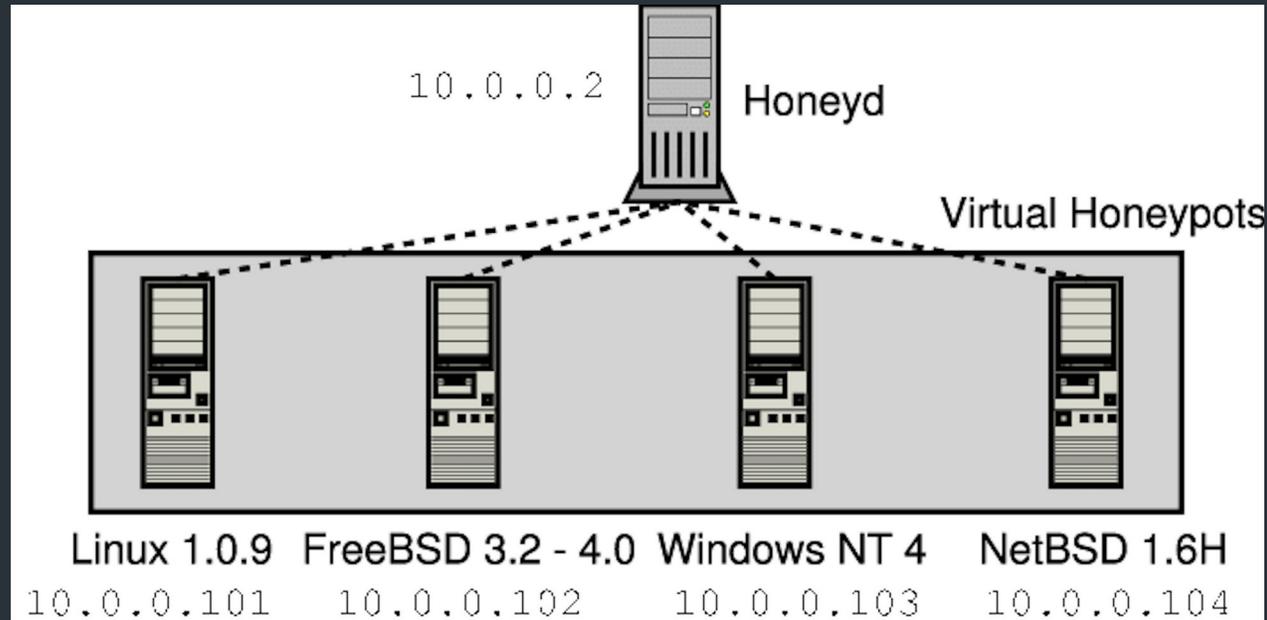
ВОЗМОЖНОСТИ

- Имитирует различные ОС
- Выполняет скрипты-заготовки для имитации shell
- Может подменять SSH-баннеры
- Позволяет запускать несколько инстансов с различными IP

ПРОТОКОЛЫ

- SSH
- FTP
- HTTPS
- TELNET
- OS
- MTP

HONEYD. DEEP DIVE



ОСОБЕННОСТИ

- Нет UI – готовим скрипты и конфиги
- Один MAC-адрес для всех сервисов
- 1 порт – 1 .sh скрипт
- Сложно дорабатывать и расширять функционал
- Требуется служба arpd
- Не является enterprise-решением, больше подходит для учебных целей

COWRIE

The screenshot shows the GitHub repository page for `cowrie/cowrie`. The repository is described as a "SSH/Telnet Honeypot" and has a URL of `https://cowrie.readthedocs.io`. It has 4.6k stars, 123 watchers, and 815 forks. The repository is written in Python (98.5%) and other languages (1.5%). The repository is updated 18 hours ago. The repository is categorized with tags: `ssh`, `security`, `honeypot`, `telnet`, and `sftp`. The repository has 140 contributors, including 129 other contributors.

cowrie/cowrie
Cowrie SSH/Telnet Honeypot
<https://cowrie.readthedocs.io>

4.6k stars · 123 watching · 815 forks

ssh security honeypot telnet sftp

Python · 4.6k · Updated 18 hours ago

Contributors 140

Languages

- Python 98.5%
- Other 1.5%

+ 129 contributors

ВОЗМОЖНОСТИ

- Подмена prompt и banner
- Имитация выполнения команд shell
- Поддержка ложной файловой системы
- Большое количество интеграций и возможности гибкого добавления собственных
- Поддерживает интеграцию с фреймворками (например MHN)

ПРОТОКОЛЫ

- SSH
- SFTP
- SCP
- TELNET

COWRIE. DEEP DIVE

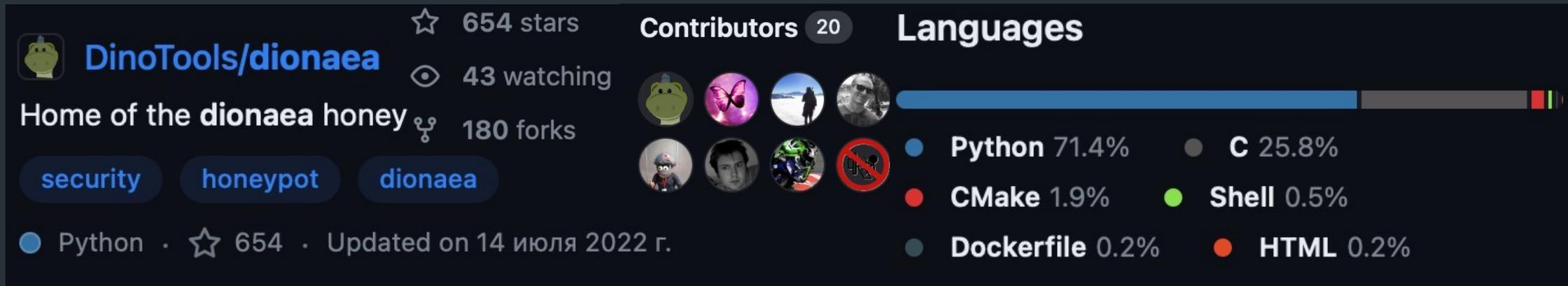
ДОСТОИНСТВА

- Продуманная архитектура
- Большое комьюнити разработчиков
- Высокоинтерактивность пользовательских сессий
- Лучший в эмуляции SSH/Telnet-сервисов

НЕДОСТАТКИ

- Ограниченное количество протоколов
- Не имитирует различные ОС
- Форки могут содержать бэкдоры — необходимо ревьюить и сканировать зависимости

DIONAEA



DinoTools/dionaea
Home of the dionaea honey

654 stars
43 watching
180 forks

Contributors 20

Languages

- Python 71.4%
- C 25.8%
- CMake 1.9%
- Shell 0.5%
- Dockerfile 0.2%
- HTML 0.2%

Python · 654 · Updated on 14 июля 2022 г.

ВОЗМОЖНОСТИ

- Возможность захвата сетевого трафика
- Поддерживает IPv6 и TLS
- Записывает действия злоумышленника
- Имитирует выполнение команд в shell
- Поддерживает интеграцию с Cuckoo, VT и MHN

ПРОТОКОЛЫ

- SMB
- FTP
- HTTPS
- TELNET
- MongoDB
- MSSQL
- MySQL
- DNS
- PPTP
- TFP
- MQTT
- MEMCACHE
- BLACKHOLE
- SIP
- NTP

DIONAEA. DEEP DIVE

ДОСТОИНСТВА

- Передает загружаемые файлы в VT
- Записывает поведение для последующего анализа
- Модульная архитектура
- Поддерживает IPv6 и TLS

НЕДОСТАТКИ

- Является коллекцией ханипотов, но не фреймворком
- Необходимо писать нормализации
- Выдает большое количество инцидентов по итогам quick scan nmap
- Все протоколы написаны различными контрибьютерами без строгих правил
- Работает менее стабильно (по сравнению с Cowrie)
- Отсутствует стабильное комьюнити для поддержки и развития проекта

Впечатление: 6/10

Поговорим о honeypot-фреймворках

HONEYTRAP

The screenshot shows the GitHub repository page for `honeytrap/honeytrap`. The repository is described as an "Advanced Honeytrap framework" and is categorized under `security`, `framework`, and `honeypot`. It has 1.1k stars, 48 watchers, and 184 forks. The repository was updated yesterday. The contributors section shows 14 contributors, with a bar chart indicating that 99.8% of the code is written in Go and 0.2% in other languages.

honeytrap/honeytrap
Advanced Honeytrap framework.

security framework honeypot

Go · 1.1k · Updated yesterday

Readme
View license
Activity
1.1k stars
48 watching
184 forks
Report repository

Contributors 14

+ 3 contributors

Languages

Go 99.8% Other 0.2%

ВОЗМОЖНОСТИ

- Управляет ловушками с низким и высоким уровнем интерактивности
- Расширяется существующими ловушками (например, Cowrie)
- Поддерживает скриптовые языки (Lua, Python, Ruby) для создания пользовательского поведения и ответов
- Фильтрует и отправляет события в топик Apache kafka/rabbitmq, индекс Elasticsearch, Splunk, file

ВНЕДРЕНИЕ

- Состоит из трех компонентов: `honeytrap-pot`, `honeytrap-agent` и `honeytrap-portal`
- Настраивается с помощью YAML-файла или веб-интерфейса

HONEYTRAP. DEEP DIVE

ДОСТОИНСТВА

- Представляет собой центральный сервер и Honeytrap Agents
- Использует агентов для перенаправления трафика
- Гибкое добавление ханипотов
- Использует свои реализации ложных сервисов

НЕДОСТАТКИ

- Ограниченные возможности управления ханипотами
- Использует LXC для поднятия контейнеров
- Нет высокоинтерактивных ханипотов

Впечатление: 7/10

T-POT

telekom-security/tpotce

T-Pot - The All In One Honeypot

5.3k stars

179 watching

898 forks

Contributors 19

Languages

- C 43.8%
- Shell 30.1%
- Dockerfile 15.6%
- GLSL 7.4%
- HCL 3.0%
- Makefile 0.1%

docker network-security elk security honeypot

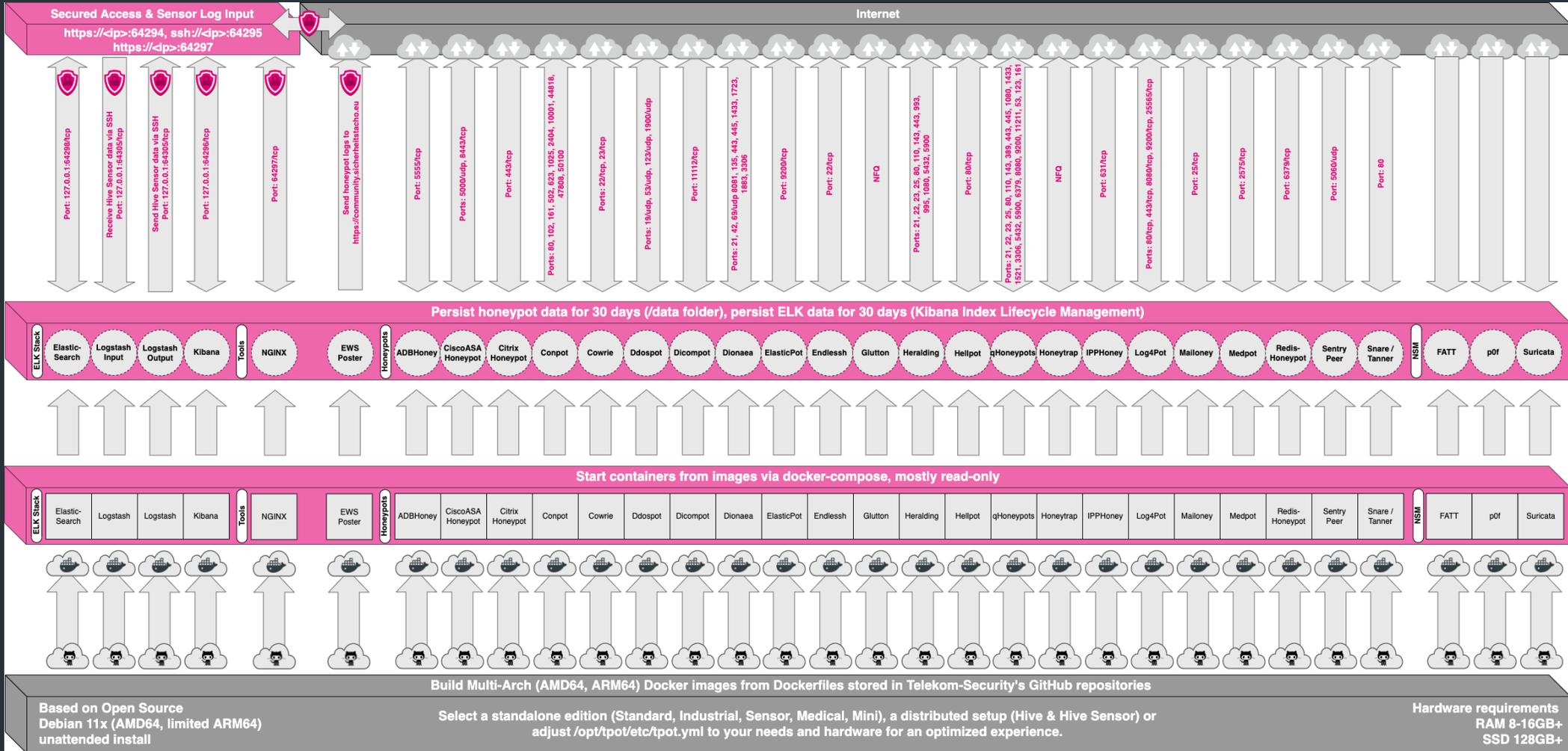
ВОЗМОЖНОСТИ

- Позволяет создавать, запускать и управлять различными типами ханипотов
- Поддерживает 20+ ханипотов и бесчисленные возможности визуализации с помощью Elastic Stack
- Комбинирует ханипоты с низким и высоким уровнем интерактивности
- Может использовать существующие ханипоты (Cowrie и другие)
- Регистрирует и отправляет события в Elasticsearch, Kafka, Splunk

ВНЕДРЕНИЕ

- Состоит из трех компонентов:
 - TROT-pot — высокоинтерактивный honeypot, на котором работают сервисы и скрипты.
 - TROT-agent — компонент, перенаправляющий трафик
 - TROT-портал — веб-интерфейс для анализа и визуализации данных
- Настраивается с помощью YAML-файла или веб-интерфейса
- Нетривиальная установка и настройка системы

T-POT. DEEP DIVE



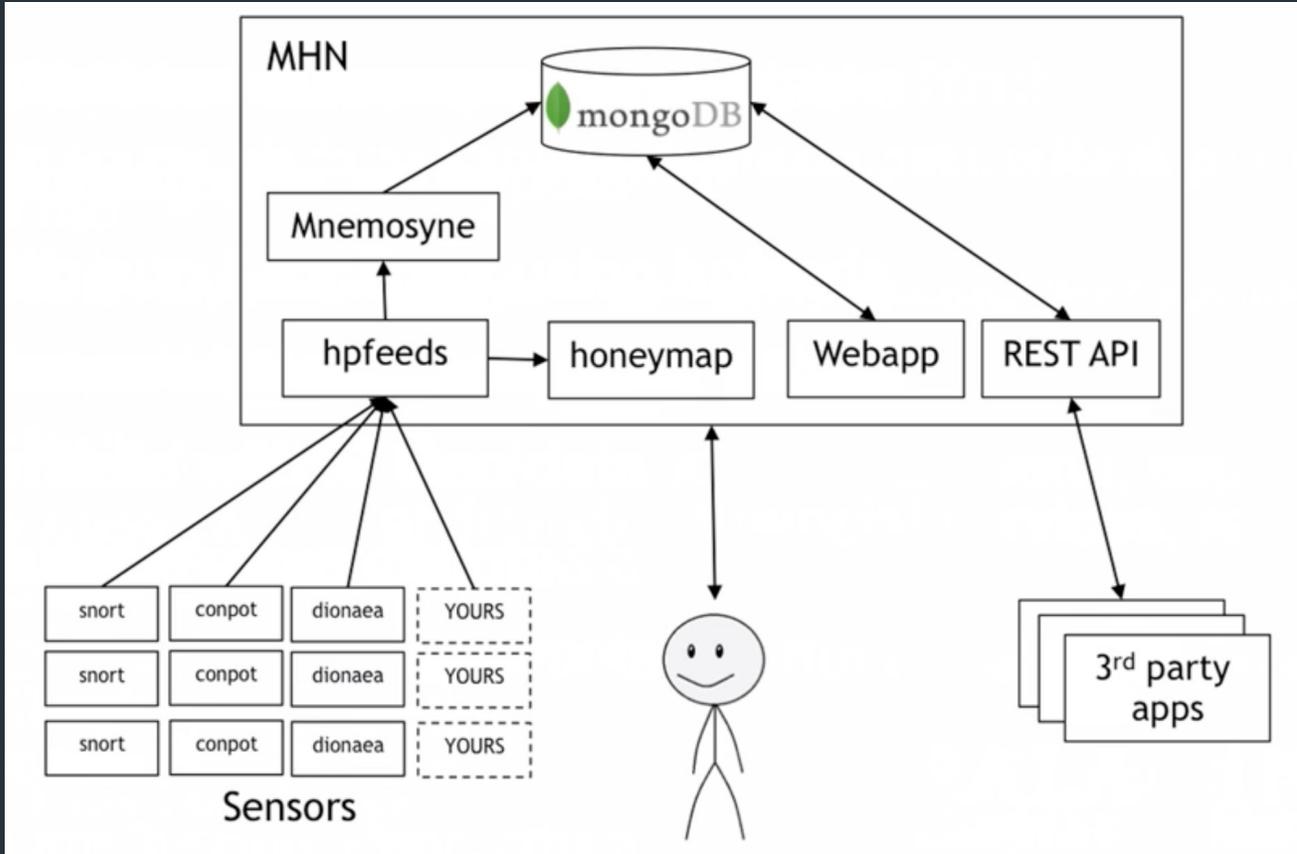


ВОЗМОЖНОСТИ

- Позволяет развертывать, контролировать и управлять различными типами ханипотов (Snort, Cowrie, Dionaea)
- Собирает и анализирует данные с ханипотов, такие как журналы атак, полезная нагрузка, сигнатуры
- Визуализирует данные с помощью графиков, карт, таблиц и отчетов

ВНЕДРЕНИЕ

- Состоит из централизованного сервера для управления ханипотами и сбора данных с них
- Поддерживает скриптовые языки, такие как Python или Bash, для создания пользовательских сценариев развертывания и парсеров
- Интегрируется с различными библиотеками и инструментами для сетевого анализа, обработки данных и визуализации



ОСОБЕННОСТИ

- Production-like подход к построению решения
- MongoDB для хранения данных
- Встроенный нормализатор сообщений (Mnemosyne) из hpfeeds
- REST API

От honeypot и фреймворков к deception

Отличительные особенности систем киберобмана от ханипотов



Экосистема ложных данных и активов на всех уровнях: сети, конечные устройства

Централизованное управление ложным слоем данных из единой консоли

Гибкие возможности интеграции с различными инфраструктурами

Адаптивная генерация: учитывается топология сети конкретной компании

Множество настроек и механик из консоли для конфигурации системы

ЭКОСИСТЕМА ЛОЖНЫХ ДАННЫХ И АКТИВОВ

Сеть

- Разной степени интерактивности ловушки, позволяющие эмулировать корпоративные системы, приложения, базы данных и другие ИТ-активы
- Сетевой трафик
- Уязвимости в сетевых устройствах (маршрутизаторы, коммутаторы и т.п)

Конечные устройства

- Учётные записи
- Сохранённые пароли в браузерах
- История команд в BASH и PowerShell
- Сохранённые SSH-ключи в хранилищах
- Ветки реестра ОС и стороннего ПО

Технологический сегмент

- Промышленное оборудование
- Программируемые логические контроллеры (ПЛК)
- АРМ-сервера
- Уязвимости в оборудовании, ПО
- Умные устройства

Платформа киберобмана

DEJAVU

bhdresh/Dejavu
DejaVU - Open Source Deception Framework

Tags: docker, honeypot, dejavu, deception, defensive-security

Languages

Language	Percentage
PHP	42.8%
JavaScript	16.3%
HTML	1.4%
Less	26.5%
CSS	12.8%
Hack	0.2%

Contributors 5

6.1k stars
262 watching
1.4k forks

ВОЗМОЖНОСТИ

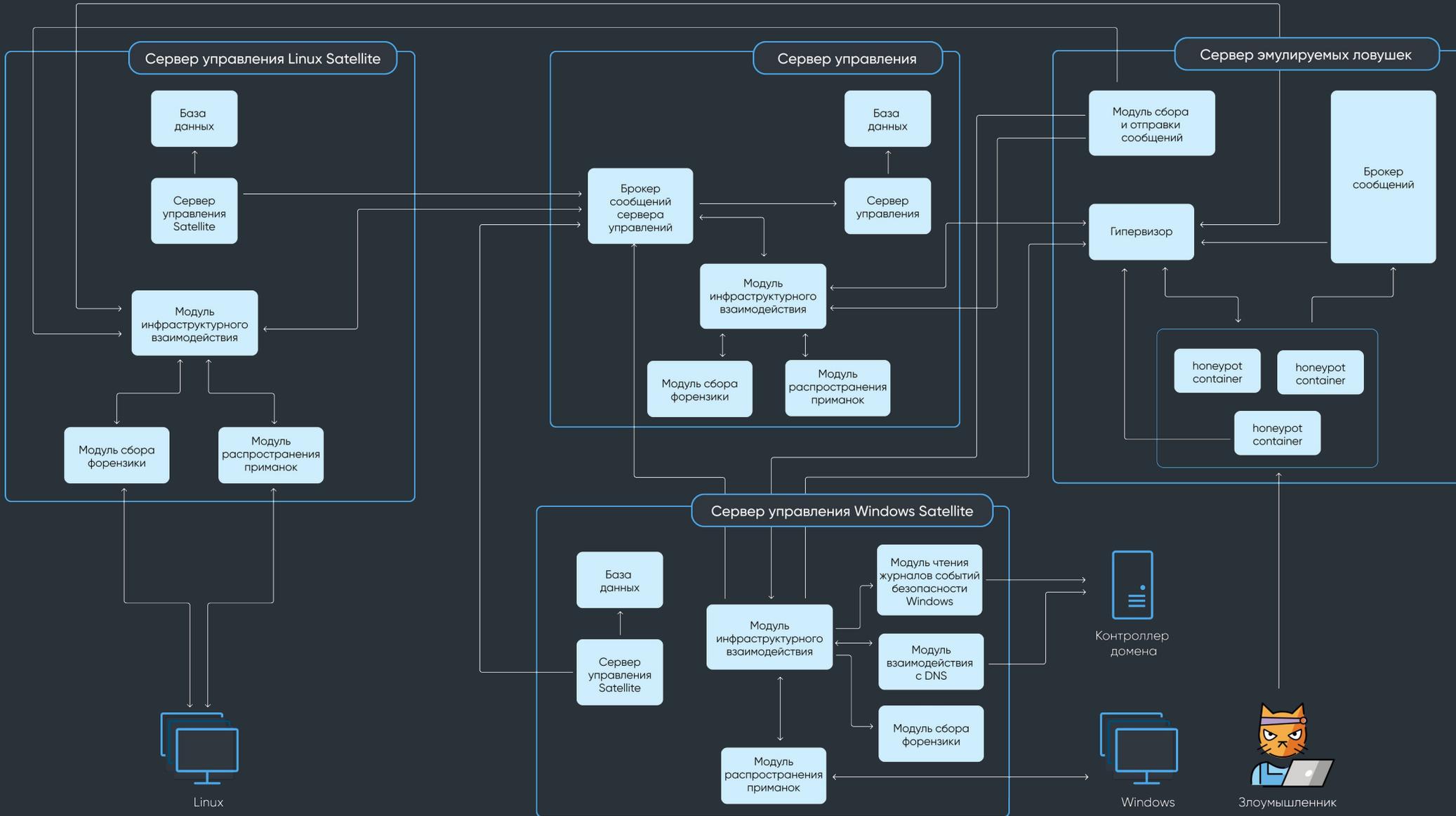
- Позволяет создавать, запускать и управлять различными типами приманок и ханипотов в сетевой инфраструктуре
- Использует существующие ханипоты (Cowrie и другие)
- Комбинирует ловушки с низким и высоким уровнем интерактивности
- Позволяет отправлять события в Elasticsearch, Kafka, Splunk

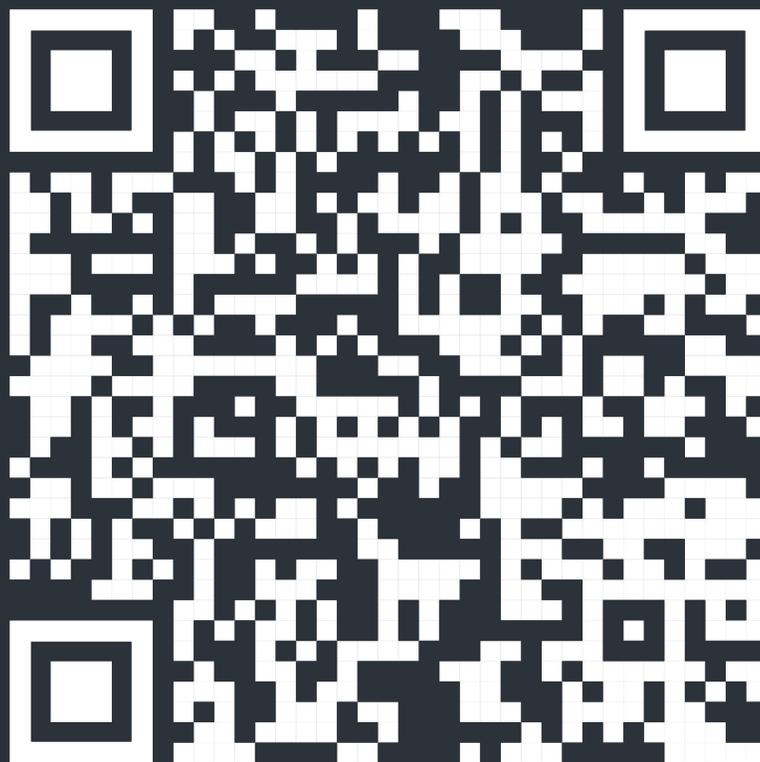
ВНЕДРЕНИЕ

- Состоит из трех компонентов:
 - Console — это веб-интерфейс и API для управления приманками, ловушками и данными
 - Engine — компонент, который разворачивает и запускает ловушки
 - Portal — компонент, который получает и хранит данные от ловушек
- Настраивается с помощью YAML-файла или веб-интерфейса

К чему пришли мы

АРХИТЕКТУРА XELLO DECEPTION





+ 7 (499) 842-90-90
info@xello.ru