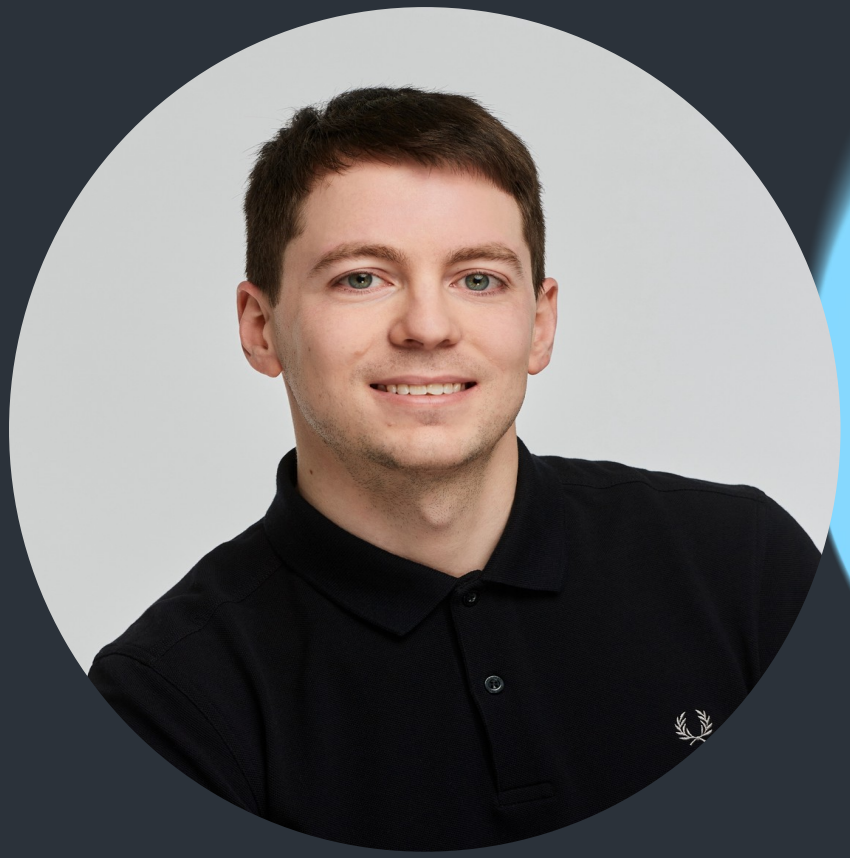
SOC
FORUM
2023

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

Дмитрий Асташкин
Дмитрий Черников

Москва, 2023

SOC
FORUM
2023



Дмитрий Асташкин

Дмитрий Черников

XELLO

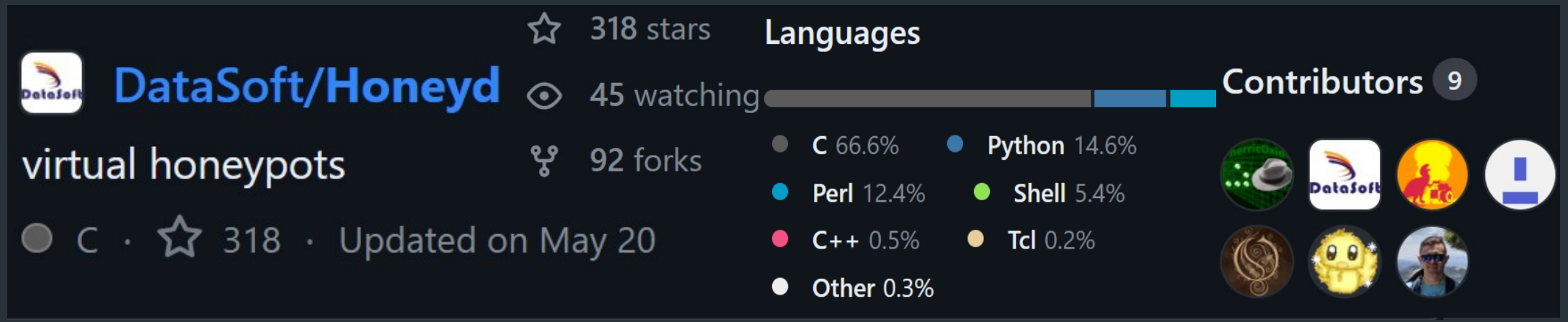
SOC FORUM 2023

Сколько Open Source-проектов ханипотов на GitHub?

4 000+

Поговорим о honeypot

HONEYD



ВОЗМОЖНОСТИ

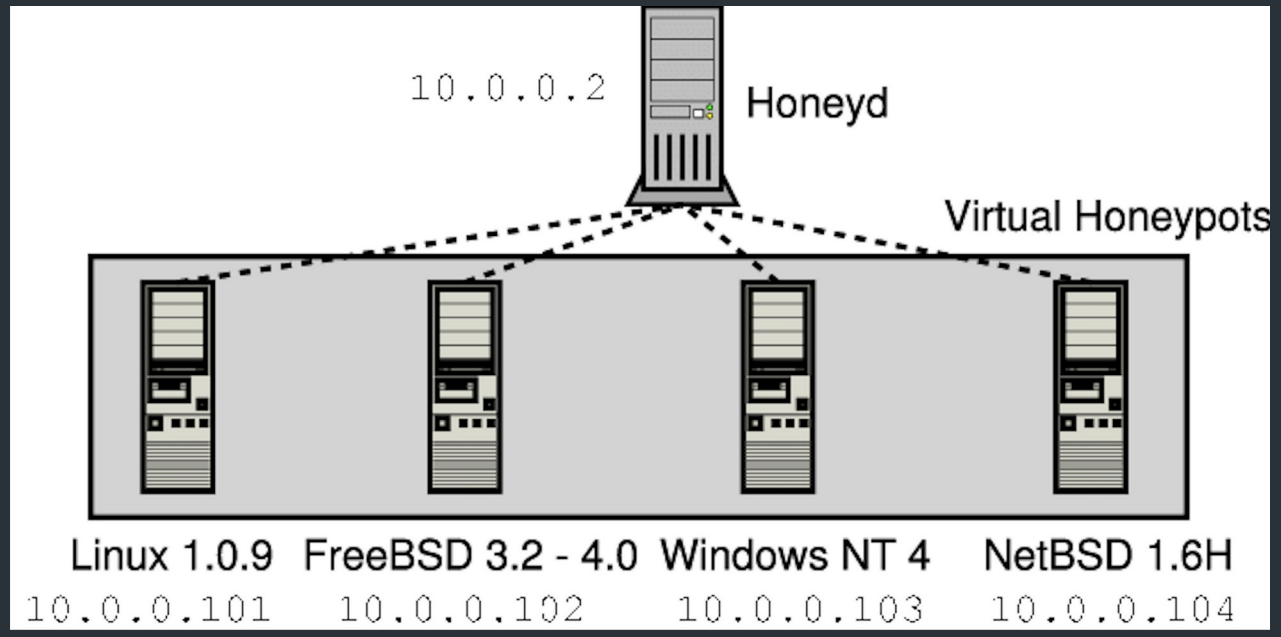
- Имитирует различные ОС
- Выполняет скрипты-заготовки для имитации shell
- Может подменять SSH-баннеры
- Позволяет запускать несколько инстансов с различными IP

ПРОТОКОЛЫ

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

HONEYD. DEEP DIVE

SOC FORUM 2023



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

Впечатление: 6/10

COWRIE

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

SOC FORUM 2023

ДОСТОИНСТВА

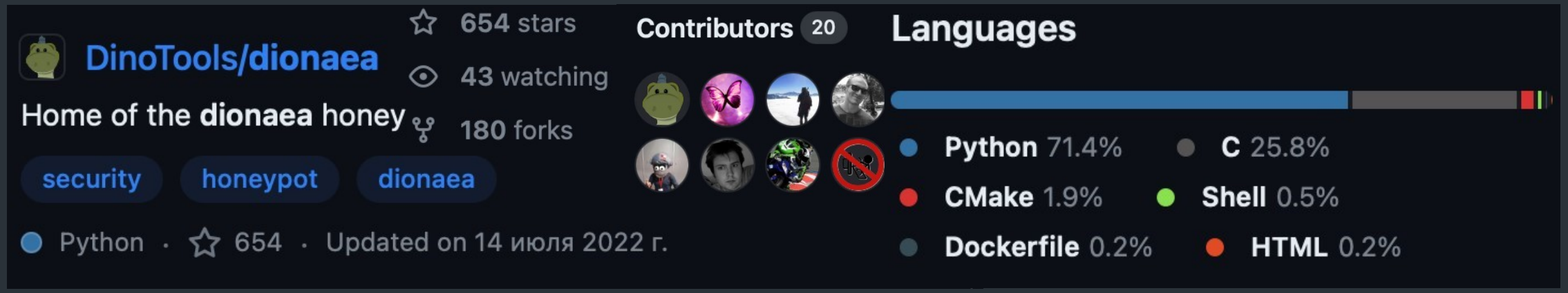
- Продуманная архитектура
- Большое комьюнити разработчиков
- Высокоинтерактивность пользовательских сессий
- Лучший в эмуляции SSH/Telnet-сервисов

НЕДОСТАТКИ

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

Впечатление: 8/10

DIONAEA



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
- MQQT
- MEMCACHE
- BLACKHOLE
- SIP
- NTP

DIONAEA. DEEP DIVE

SOC FORUM 2023

ДОСТОИНСТВА

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

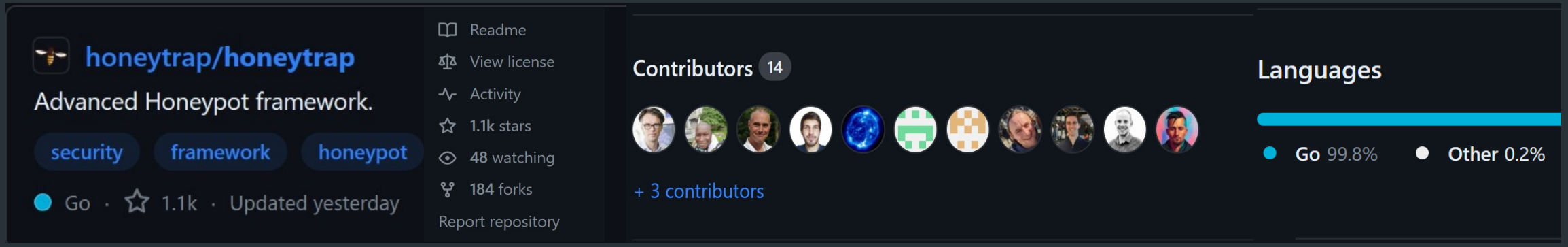
НЕДОСТАТКИ

- 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



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/rabbirmq, 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

SOC FORUM 2023

ДОСТОИНСТВА

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

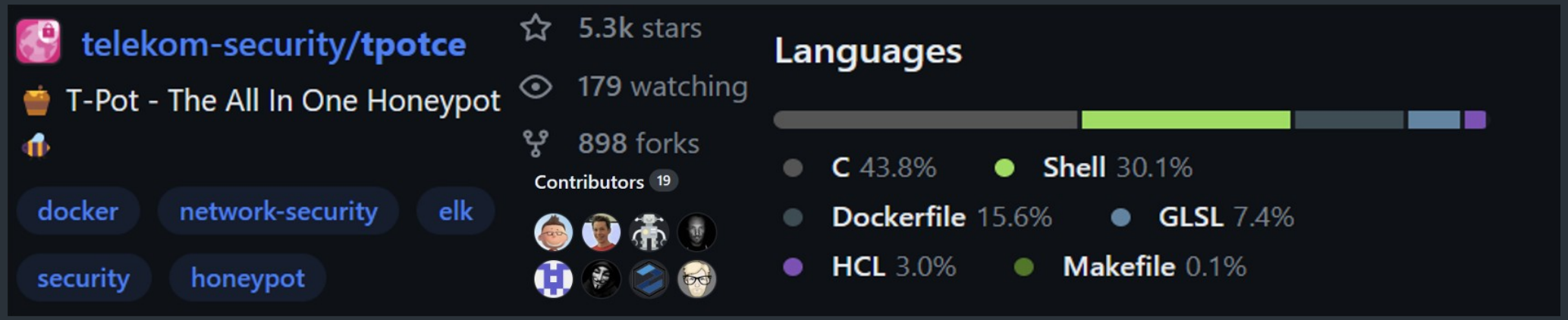
НЕДОСТАТКИ

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

Впечатление: 7/10

SOC FORUM 2023

T-POT



ВОЗМОЖНОСТИ

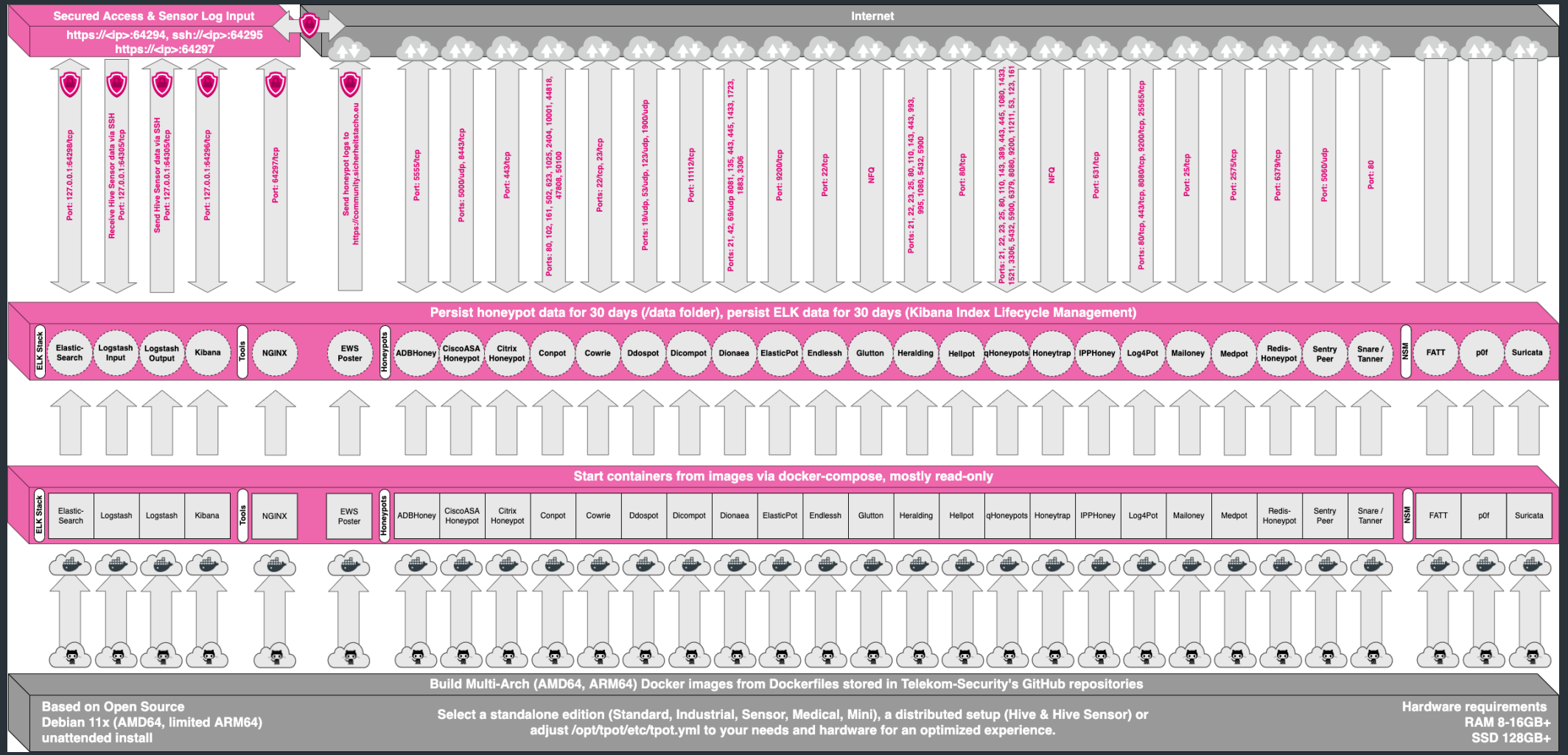
- Позволяет создавать, запускать и управлять различными типами ханипотов
- Поддерживает 20+ ханипотов и бесчисленные возможности визуализации с помощью Elastic Stack
- Комбинирует ханипоты с низким и высоким уровнем интерактивности
- Может использовать существующие ханипоты (Cowrie и другие)
- Регистрирует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

ВНЕДРЕНИЕ

- Состоит из трех компонентов:
  - TPOT-pot — высокоинтерактивный honeypot, на котором работают сервисы и скрипты.
  - TPOT-agent — компонент, перенаправляющий трафик
  - TPOT-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

SOC FORUM 2023



Впечатление: 6/10

MHN

ВОЗМОЖНОСТИ

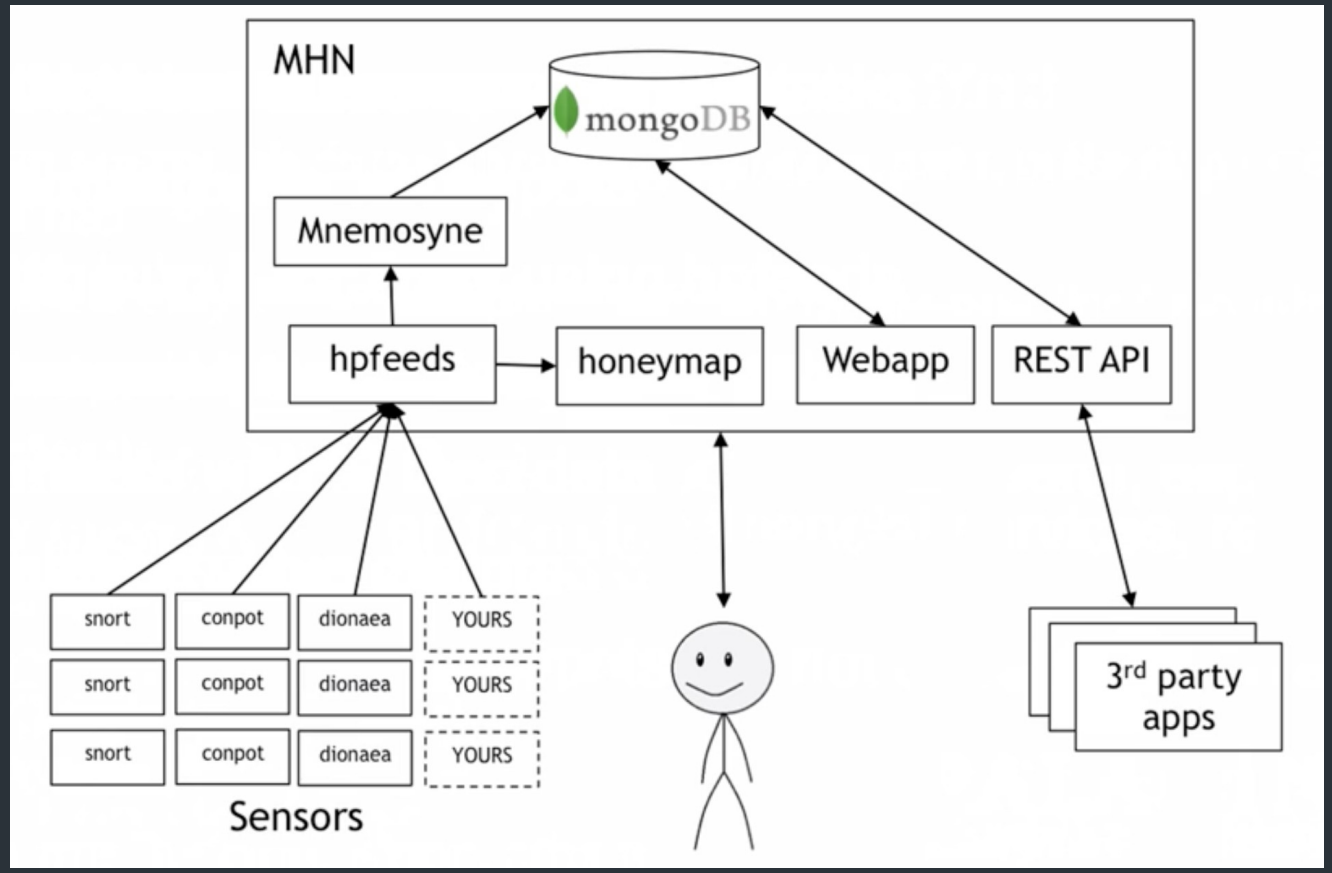
- Позволяет развертывать, контролировать и управлять различными типами ханипотов (Snort, Cowrie, Dionaea)
- Собирает и анализирует данные с ханипотов, такие как журналы атак, полезная нагрузка, сигнатуры
- Визуализирует данные с помощью графиков, карт, таблиц и отчетов

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

MHN. DEEP DIVE

SOC FORUM 2023



ОСОБЕННОСТИ

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

Впечатление: 8/10

От honeypot
и фреймворков к deception

Отличительные особенности систем киберобмана от ханипотов

SOC FORUM 2023

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

SOC FORUM 2023

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

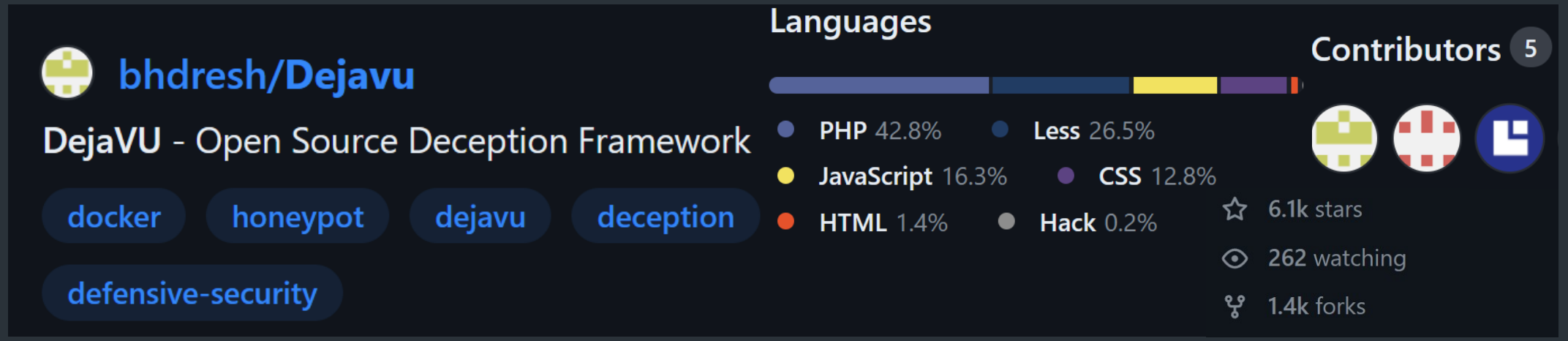
Технологический сегмент

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

Платформа кибероbмана

SOC FORUM 2023

DEJAVU



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

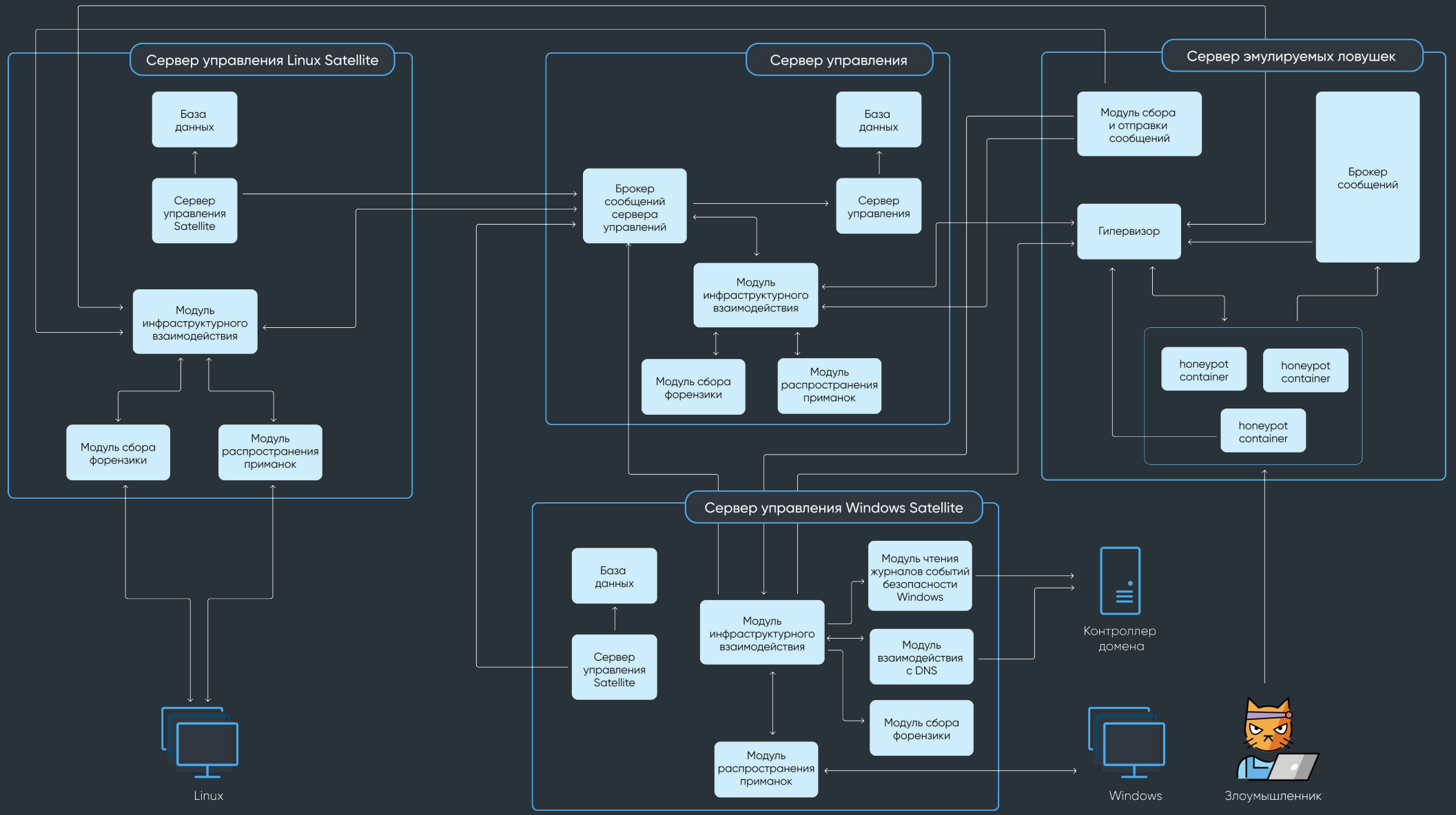
ВНЕДРЕНИЕ

- 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

SOC FORUM 2023



xello

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