ПРОЕКТ «ХАНИПОТ»

ЦЕЛИ ИСПОЛЬЗОВАНИЯ ХАНИПОТОВ

Внедрить системы на стратегическом уровне

Внедрить в национальную инфраструктуру кибербезопасности

Обеспечить защиту критически важных информационных активов

Способствовать достижению стратегических целей в области обеспечения безопасности страны

СПОСОБЫ ДОСТИЖЕНИЯ ЦЕЛЕЙ

Обнаружение и анализ угроз

Усиление защиты критически важной инфраструктуры

Исследование и сбор информации

Межведомственное и международное сотрудничество

ХАНИПОТ

- Ханипоты — это специализированная система-ловушка, предназначенные для имитации реальных компьютерных систем.
- Такие системы:
  - Не содержат никаких ценных данных
  - Настраиваются для изучения активности злоумышленника в сети
  - Создаются, чтобы создавать более надежные средства защиты за счёт регистрации событий и сетевого трафика
  - Позволяют не только обнаруживать и анализировать кибератаки
  - Позволяют предсказывать новые угрозы
  - Повышают общую киберустойчивость государств и организаций.

ПРИМЕРЫ АТАК И УЯЗВИМОСТЕЙ КОТОРЫЕ ХАНИПОТЫ ПОМОГАЮТ ОБНАРУЖИВАТЬ И АНАЛИЗИРОВАТЬ

- Инъекции
- DDoS-атаки
- Сетевые вторжения и уязвимости сетевых протоколов
- Атаки через почтовые сервисы
- Уязвимости операционных систем
- Уязвимости серверного программного обеспечения
- Уязвимости в конфигурации
- Zero-Day уязвимости
- Выявление вредоносного программного обеспечения

ОБМЕН ДАННЫМИ

- Также концепция обмена данными может поддерживать проведение регулярных киберучений, включающих различные государственные органы, организации и других партнёров
- Проверка готовности и эффективности реагирования на киберинциденты
- Возможно сотрудничество в регионе.

ПОДКЛЮЧЕНИЕ К ГЛОБАЛЬНЫМ ПЛАТФОРМАМ

- Реализация проекта может помочь Кыргызской Республики интегрировать свои данные в глобальные платформы кибербразведки, такие как:
  - ISACs (Information Sharing and Analysis Centers)
  - другие международные инициативы
- Поспособствует более широкому распространению информации об угрозах в своей области
- Поддержит коллективный отклик на общие угрозы

ОСНОВНЫЕ КОМПОНЕНТЫ

Tpot-Hive

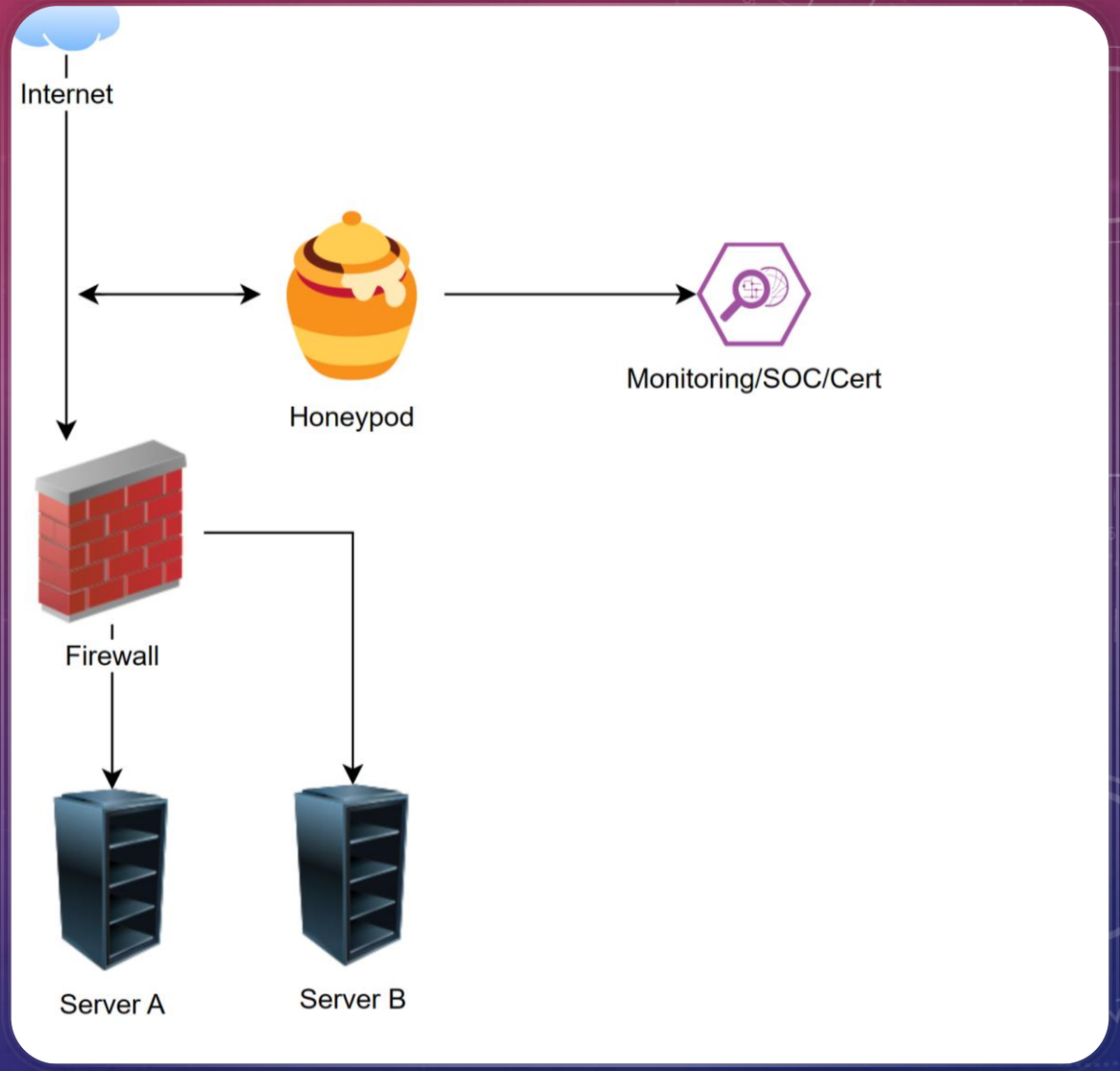
Tpot-Sensor

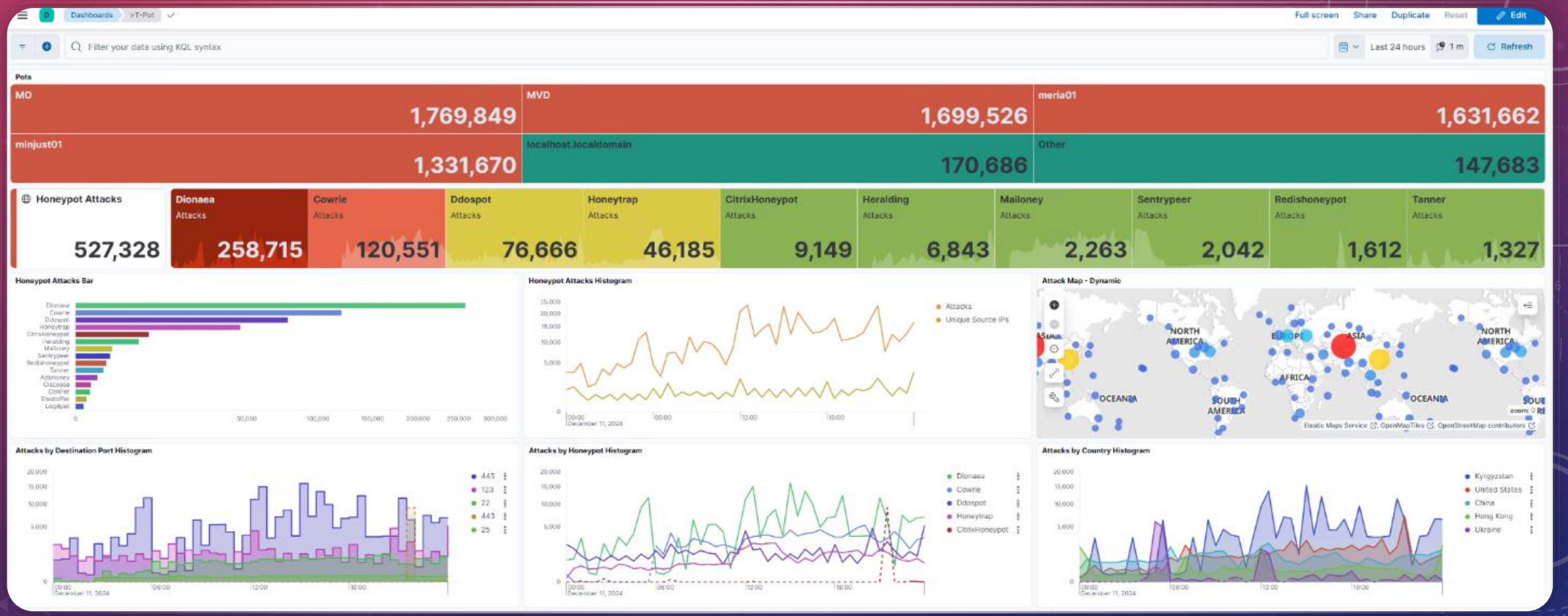
RTIR

MISP

СХЕМА УСТАНОВКИ ХАНИПОТ В ОРГАНИЗАЦИИ

- Системы ханипот работают изолированно от сети организаций
- Установка произведена до межсетевого экрана
- Система не снижает общую безопасность организации в случае взлома
- Системы установлены на:
  - физические сервера
  - в качестве виртуальной машины




Dashboards
>T-Pot
Full screen
Share
Duplicate
Reset
Edit
Filter your data using KQL syntax
Last 24 hours
1 m
Refresh
Pots
MO
1,769,849
MVD
1,699,526
meria01
1,631,662
minjust01
1,331,670
localhost.localdomain
170,686
Other
147,683
Honeypot Attacks
527,328
Dionaea
Attacks
258,715
Cowrie
Attacks
120,551
Ddospot
Attacks
76,666
Honeytrap
Attacks
46,185
CitrixHoneypot
Attacks
9,149
Heralding
Attacks
6,843
Mailoney
Attacks
2,263
Sentrypeer
Attacks
2,042
Redishoneypot
Attacks
1,612
Tanner
Attacks
1,327
Honeypot Attacks Bar
Honeypot Attacks Histogram
Attacks
Unique Source IPs
Attack Map - Dynamic
NORTH AMERICA
EUROPE
ASIA
AFRICA
OCEANIA
SOUTH AMERICA
Elastic Maps Service
OpenMapTiles
OpenStreetMap contributors
Attacks by Destination Port Histogram
445
123
22
443
25
Attacks by Honeypot Histogram
Dionaea
Cowrie
Ddospot
Honeytrap
CitrixHoneypot
Attacks by Country Histogram
Kyrgyzstan
United States
China
Hong Kong
Ukraine


type.keyword:"Suricata"
Last 24 hours
Refresh
Suricata Events Bar
Events
Unique Src IPs
Unique JA3s
0
20,000
40,000
60,000
80,000
Events
Suricata Events
98,563
Events
1,273
Unique Src IPs
69
Unique JA3s
Attack Map - Dynamic
NORTH AMERICA
SOUTH AMERICA
AFRICA
ASIA
OCEANIA
zoom: 0.98
Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors
Suricata Events Histogram
Events
Unique Src IPs
Unique JA3s
Events
Timestamp
06:00
12:00
February 6, 2024
18:00
00:00
February 7, 2024
06:00
Suricata Alert Category Histogram
Detection of a Network ...
Attempted Denial of Ser...
Misc activity
Attempted Administrato...
Generic Protocol Comm...
Attacks
Timestamp
Suricata Destination Ports Histogram
445
53
59...
0
56...
Count
Timestamp
Suricata Events by Country Histogram
Kyrgyzs...
Ukraine
Iran
Croatia
Uruguay
Count
Timestamp
Suricata - Attacker Src IP Reputation
known attacker
bot, crawler
mass scanner
tor exit node
Suricata HTTP Hostname Pie - Top 10
213.109.67.176
103.28.32.56
103.174.73.85
hotmail-com.olc.protect...
Suricata HTTP Content Type - Top 10
text/html
application/json
application/octet-stream
text/plain
Suricata Countries - Top 10
Kyrgyzstan
Ukraine
Iran
Croatia

ОСНОВНЫЕ ПРОБЛЕМЫ ДАННОГО ПРОЕКТА

- **Обнаружение ханипот злоумышленниками**
- Злоумышленники могут обнаруживать ханипот-системы
  - анализируя их поведение,
  - проверяя наличие уязвимостей,
  - анализируя сетевой трафик,
  - информацию о хосте,
  - проводя проверки на необычные реакции.
- Они могут изучать ответы сервисов, анализировать заголовки и баннеры, и проводить тестирование на динамическое поведение, чтобы выявить характеристики, отличающие ханипот от реальных сред.

ОСНОВНЫЕ ПРОБЛЕМЫ ДАННОГО ПРОЕКТА

- **Распространение фидов с данными ханипот**
- Важным аспектом реализации является публикация данных, зафиксированных ханипотом.
- Необходимо разработать:
  - политику,
  - инструкции по категоризации и классификации,
  - требования по ограничению доступа, по которым эта информация будет отправлена в фиды или опубликована на публичных ресурсах,
  - рекомендации по применению в организациях.

ОСНОВНЫЕ ПРОБЛЕМЫ ДАННОГО ПРОЕКТА

- Ханипоты, генерируют большие объёмы телеметрии и событий, часто сложных для интерпретации. Эффективность их использования напрямую зависит от уровня подготовки аналитиков, работающих с такими системами.
- **Что требуется от специалистов:**
- • Глубокое понимание принципов работы ханипотов, включая различие между эмуляцией и симуляцией.
- • Умение анализировать и ранжировать события, выделять значимое среди большого количества сигналов.
- • Контекстуализация данных — аналитик должен понимать, в какой атаке, на каком этапе и с какими намерениями использовался тот или иной приём.
- • Решения по ложноположительным срабатываниям — необходимо чётко отличать реальные угрозы от шумов, не теряя чувствительности системы.

СПАСИБО ЗА ВНИМАНИЕ