УРАЛЬСКИЙ ЦЕНТР
СИСТЕМ БЕЗОПАСНОСТИ

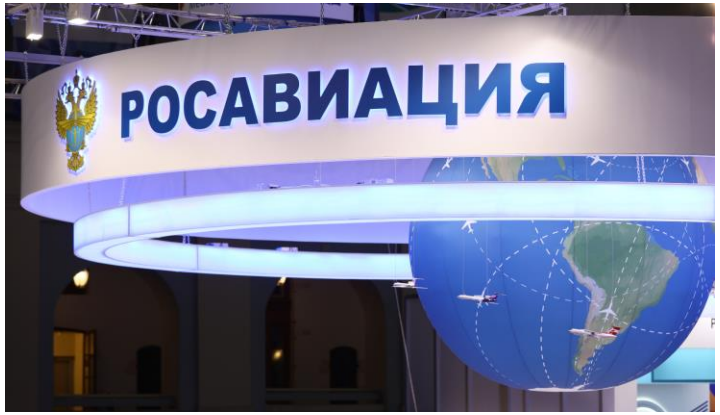
БИТ БЕЗОПАСНОСТЬ
информационных технологий
ФОРУМ – УРАЛ•2022

КАК ПОЙМАТЬ ХАКЕРА,
ЕСЛИ ОН УЖЕ ПРОНИК В СЕТЬ?

Евгений Баклушин
Старший аналитик АЦ

ХАКЕР В СЕТИ

РОСТ КОЛИЧЕСТВА ИНЦИДЕНТОВ



Росавиация подверглась хакерской атаке по схеме «человек посередине»

Нарушена работа ИТ-инфраструктуры, парализованы почта и электронный документооборот

Яндекс

Утечка в «Яндекс.Еда». В открытый доступ попали SQL-базы, суммарно содержащие около 49 миллионов строк, включая: ФИО, номера телефонов, адреса граждан РФ, Казахстана и Беларуси

МИРАТОРГ

Целенаправленная атака на ИТ-инфраструктуру. Отсутствовала система резервного копирования

Отсутствует возможность оформлять производственные и транспортные ветеринарные документы на продукцию

Нарушены цепочки поставок

ХАКЕР В СЕТИ

СТАТИСТИКА

Количество инцидентов по НКЦКИ*

589
78 недель
(27.08.20-23.02.22)

2240
1 неделя
(24.02.22-02.03.22)

1553
4 недели
(03.03.22-30.03.22)

Классификация жертв


Субъекты КИИ


Финансовый сектор


Государственный сектор


Здравоохранение


Пищевая промышленность

Категории инцидентов

- Внедрение вредоносного ПО
- Нарушение работы информационного ресурса
- НСД в систему
- Попытки НСД в систему
- Сбор сведений об объектах
- Эксплуатация уязвимостей
- Разглашение информации

*Национальный координационный центр по компьютерным инцидентам

ХАКЕР В СЕТИ

ВРЕМЯ НА РЕАГИРОВАНИЕ

101

День в среднем уходит на обнаружение инцидента

96%

На столько уменьшится ущерб, если инцидент будет выявлен в течение дня

СПОСОБЫ ОБНАРУЖЕНИЯ ИЛИ ПРЕДОТВРАЩЕНИЯ

1 Отключение информационного ресурса/сервиса	— радикальность — недоступность ресурса/сервиса
2 Мониторинг событий	— необходимы высокие компетенции — $$ (трудозатраты/закупка спецПО)
3 Подключение к Security operations center	— предварительная настройка источников событий

ХАКЕР В СЕТИ

СПОСОБЫ ОБНАРУЖЕНИЯ ИЛИ ПРЕДОТВРАЩЕНИЯ

1 Отключение информационного ресурса/сервиса	— радикальность — недоступность ресурса/сервиса
2 Мониторинг событий	— необходимы высокие компетенции — $$ (трудозатраты/закупка спецПО)
3 Подключение к Security operations center	— предварительная настройка источников событий
4 Honeypot	

HONEYPOT

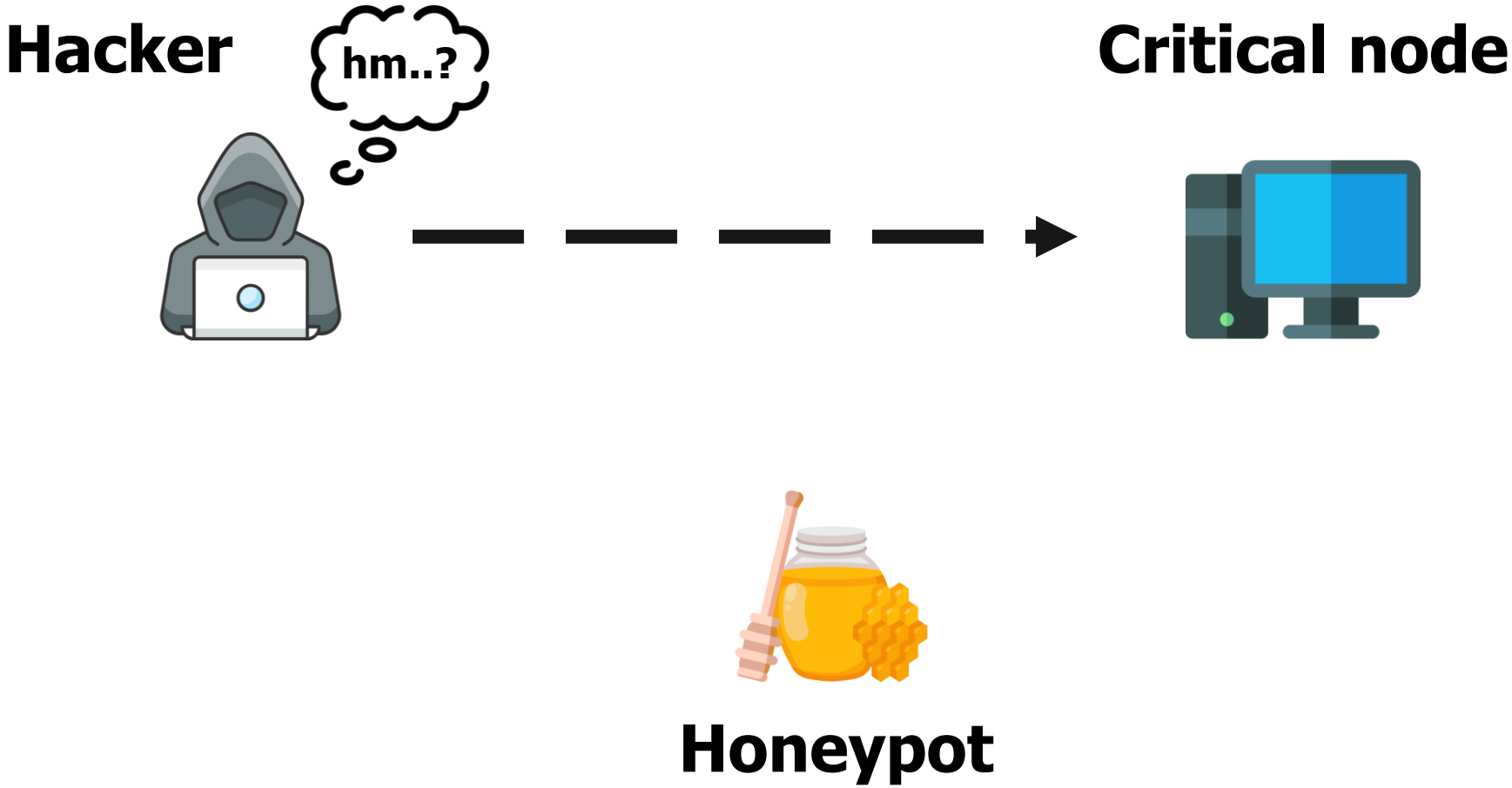
ПРИМАНКА

Hacker

Critical node

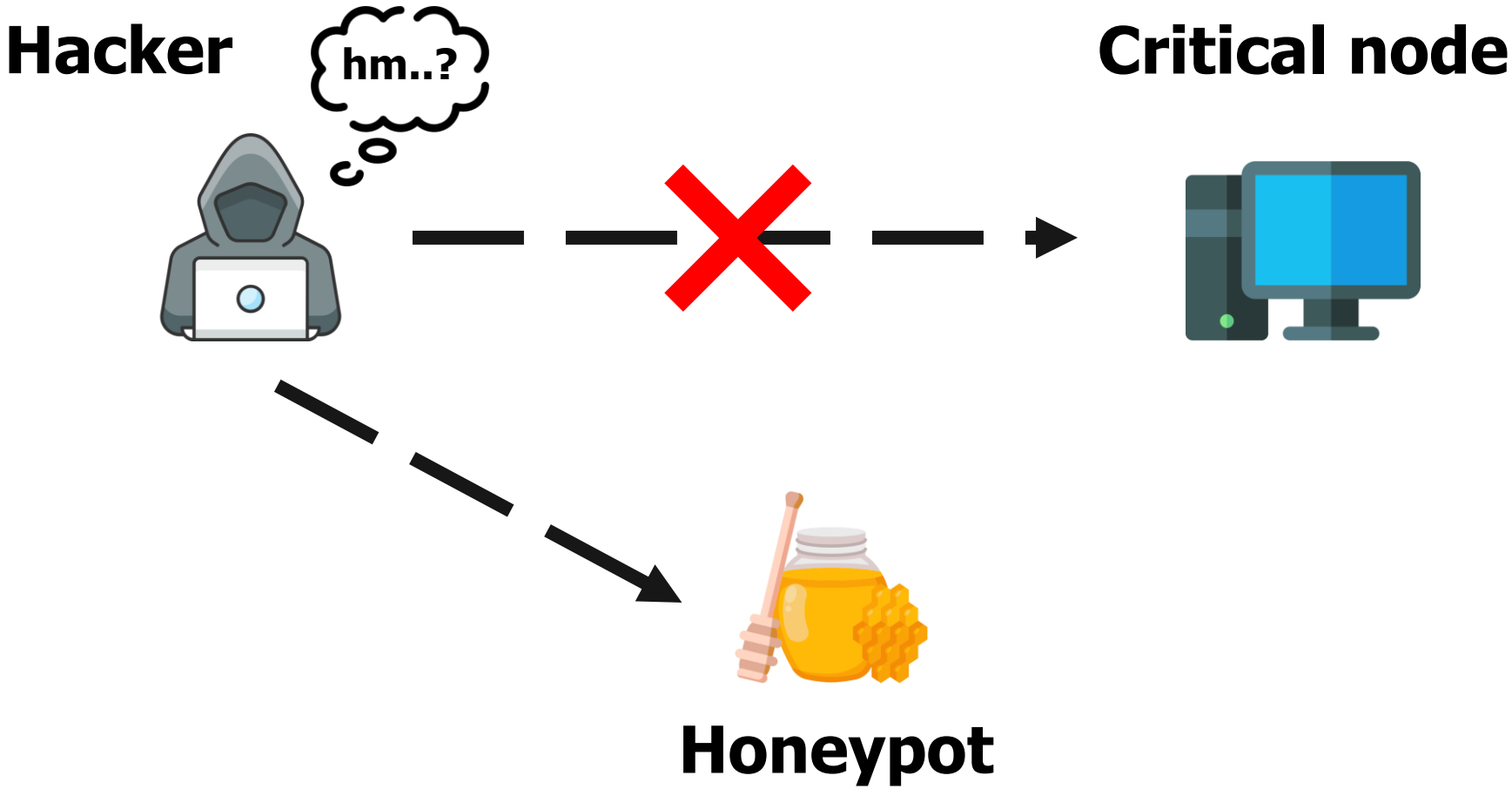
HONEYPOT

ПРИМАНКА



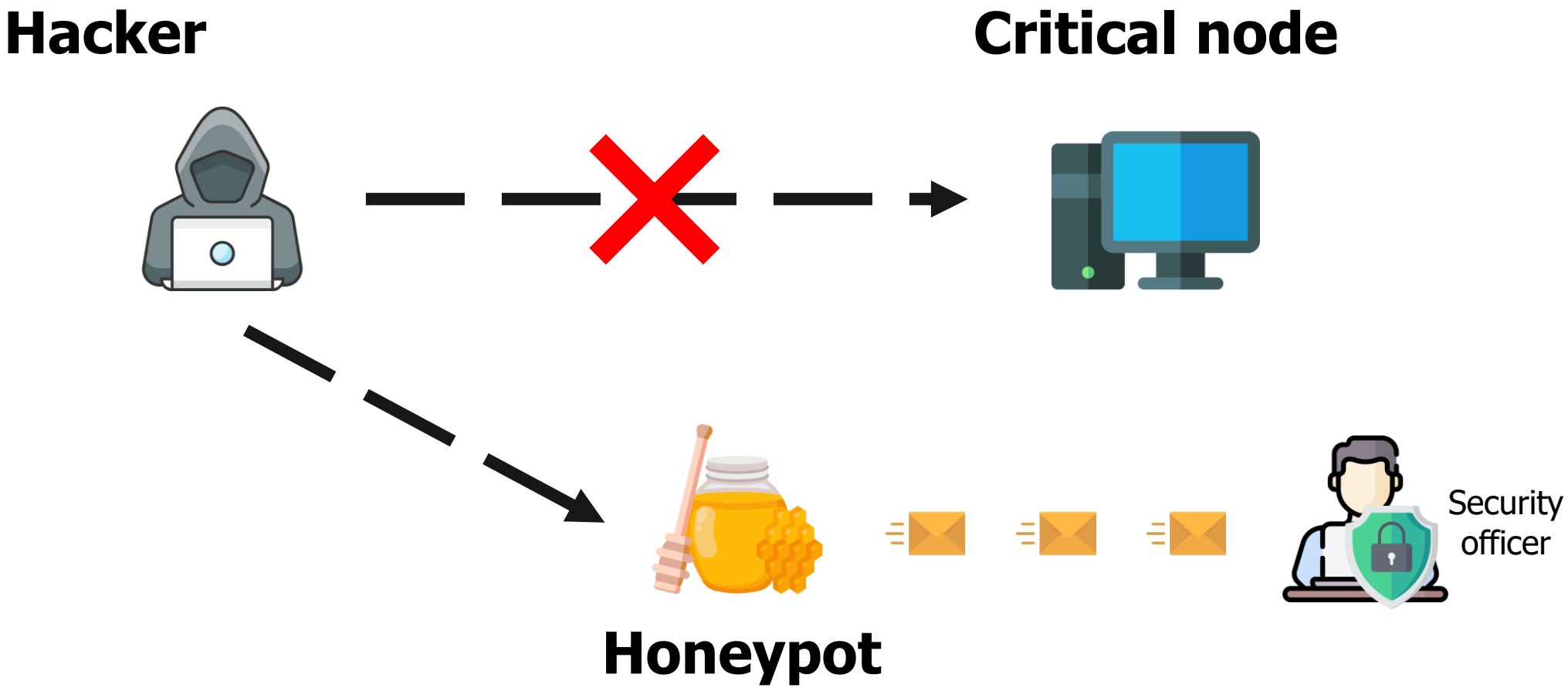
HONEYPOT

ПРИМАНКА



HONEYPOT

ПРИМАНКА



HONEYPOT

ОБЩИЕ ТРЕБОВАНИЯ

- Имитация уязвимого узла
- Наличие нескольких режимов эксплуатации
- Сбор содержательной информации
- Низкие требования к вычислительным ресурсам
- Простота установки и конфигурирования
- Наличие уведомлений

HONEYPOT.LAN

ВОЗМОЖНОСТИ

- Имитация уязвимого узла **(сервер/АРМ/АСО)**
- Наличие нескольких режимов эксплуатации **(Linux/Windows/Cisco)**
- Сбор содержательной информации **(корреляция событий)**
- Низкие требования к вычислительным ресурсам **(образ ~1 Гб)**
- Простота установки и конфигурирования **(~10 минут)**
- Наличие уведомлений **(Email/SMS)**
- **Собственный механизм обнаружения bruteforce**
- **Обнаружение распространенных сетевых атак**

HONEYPOT.LAN

ВАРИАНТЫ ИМИТАЦИИ ОС

Linux

- Обнаружение bruteforce:
  - SSH
  - MySQL
  - PostgreSQL
  - VNC

Windows

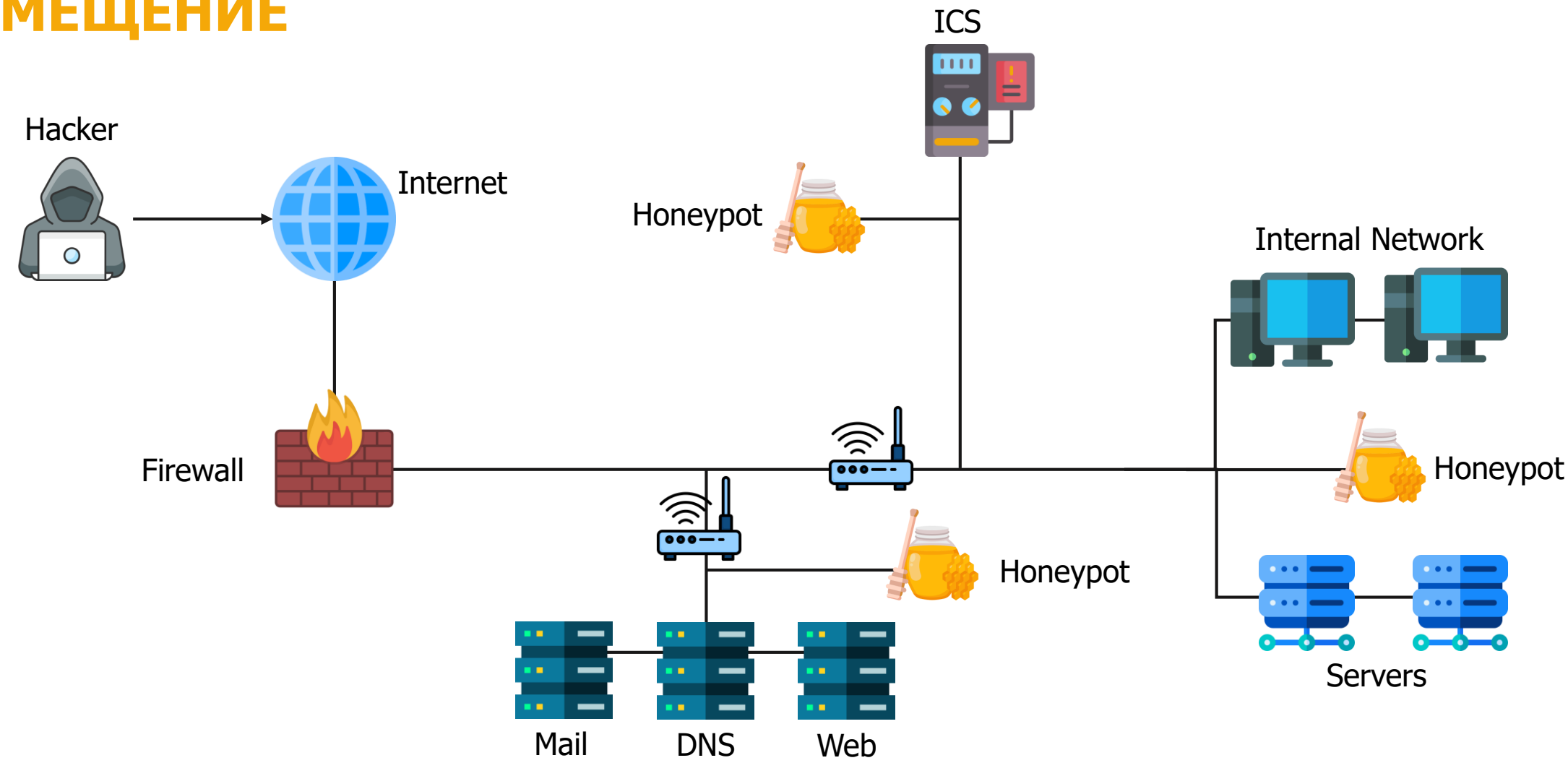
- Обнаружение bruteforce:
  - SMB
  - MSSQL
  - RDP
- Обнаружение spoofing (NetBIOS)
- Обнаружение эксплуатации MS17-010
- Обнаружение эксплуатация BlueKeep

Cisco IOS

- Обнаружение bruteforce
- Обнаружение попытки получения доступа к конфигурационному файлу (Cisco smart install)

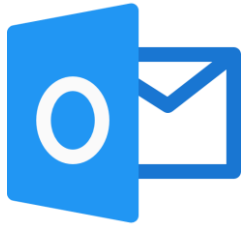
HONEYPOT.LAN

РАЗМЕЩЕНИЕ



HONEYPOT.LAN

УВЕДОМЛЕНИЯ



Письма на почту

SMS

Telegram bot

beta-test

Релиз Honeypot.Lan Community Edition в мае 2022 года

КАК ПОЙМАТЬ ХАКЕРА?

DAT APK

Мониторинг ИБ АСУ ТП

USSC SOC

Разбор инцидентов ИБ и уведомление НКЦКИ

Тестирование на проникновение

USSC

СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

Евгений Баклушин

Старший аналитик

Аналитический центр

compliance@ussc.ru

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ

БИТ БЕЗОПАСНОСТЬ информационных технологий ФОРУМ – УРАЛ•2022