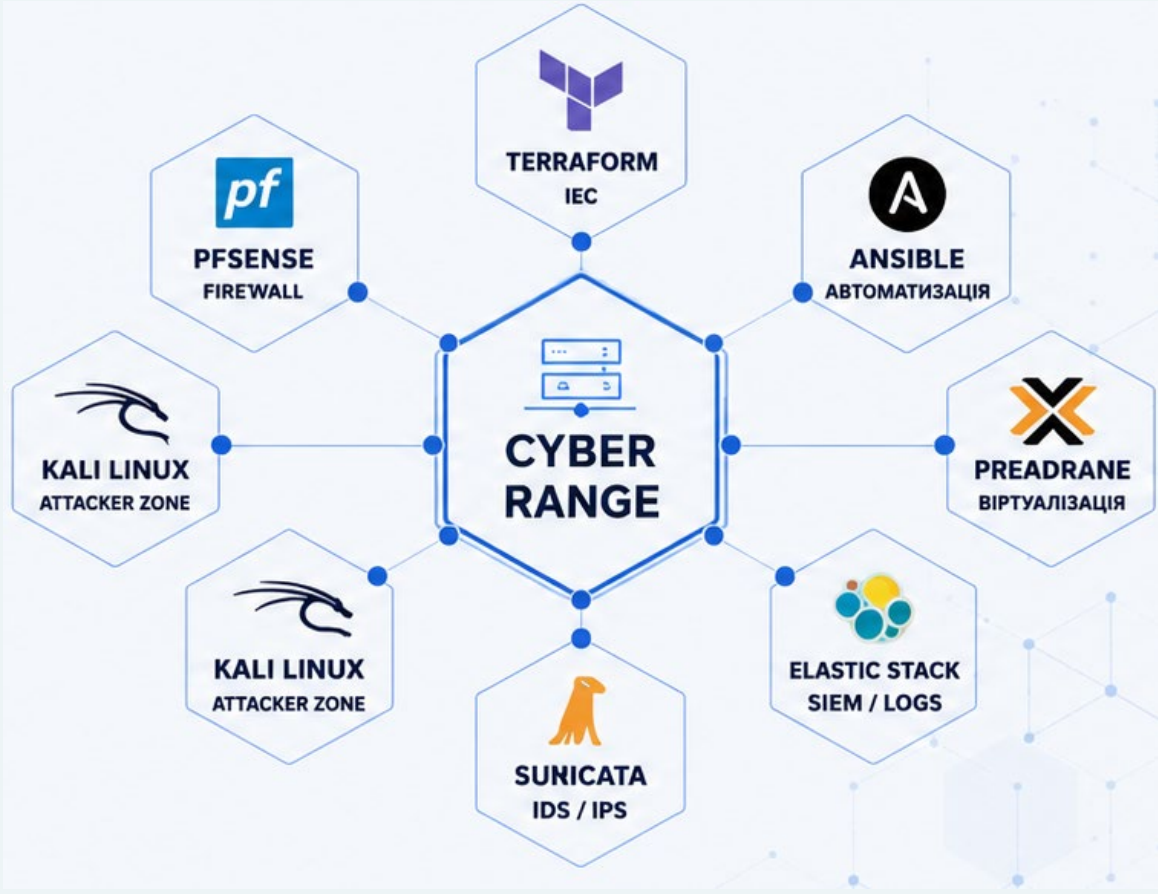
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Київський національний університет будівництва і архітектури

КВАЛІФІКАЦІЙНА ВИПУСКНА РОБОТА

Кіберполігон для дослідження мережевих атак на корпоративну інфраструктуру



Спеціальність: 123 «Комп’ютерна інженерія»

Освітня програма: Комп’ютерні системи і мережі

Виконала: Павлюк Каріна Вікторівна

Науковий керівник: Делембовський Максим Михайлович

Київ — 2026

ВСТУП

Актуальність теми

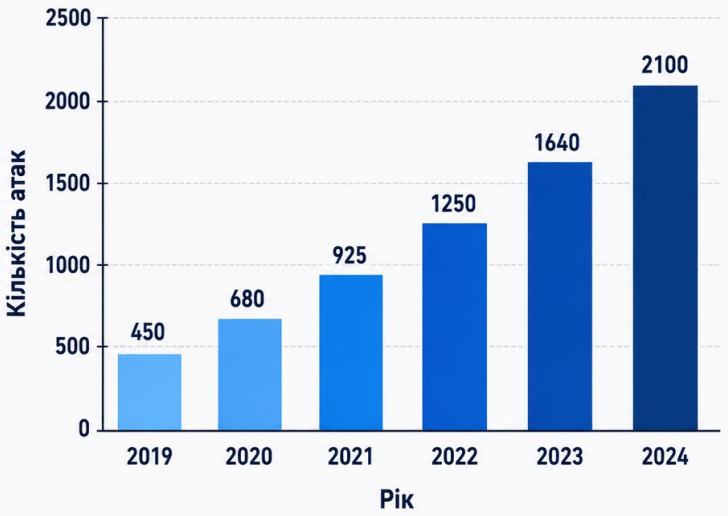
×4,6 зростання кількості атак на корпоративні мережі у 2019–2024 рр.

$4,45 млн середня вартість одного кіберінциденту (IBM, 2024)

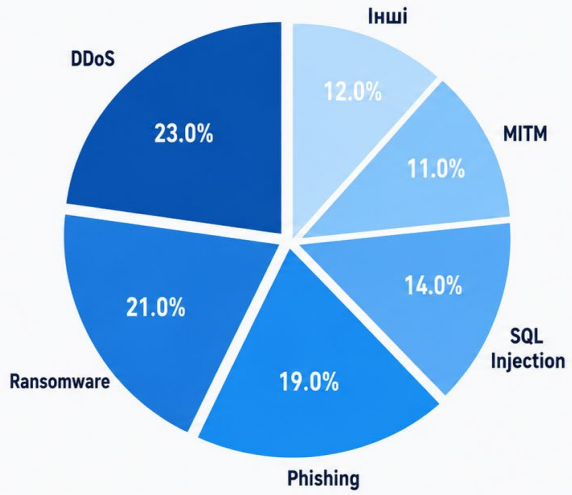
> 4 млн світовий дефіцит фахівців з кібербезпеки (ISC²)

1500+ значущих кіберінцидентів зафіксовано CERT-UA у 2023–2024

Середньотижнева кількість атак на корпоративні мережі (на 1 організацію)



Розподіл типів кібератак на корпоративні мережі (2024)



> Стрімке зростання складності й кількості мережевих атак робить практичну підготовку фахівців у безпечному, реалістичному середовищі **критично важливою.**

ВСТУП

Мета, об’єкт і предмет дослідження

МЕТА РОБОТИ

Проектування та реалізація кіберполігона на основі відкритого ПЗ і віртуалізації для дослідження мережевих атак на корпоративну інфраструктуру та оцінки ефективності засобів виявлення й протидії.

ОБ’ЄКТ ДОСЛІДЖЕННЯ

Процеси виявлення та дослідження мережевих атак у корпоративних комп’ютерних мережах.

ПРЕДМЕТ ДОСЛІДЖЕННЯ

Кіберполігон як апаратно-програмний комплекс для моделювання атак в ізольованому середовищі, що відтворює копроративну інфраструктуру.

Методи: системний і порівняльний аналіз, проектування комп’ютерних мереж, моделювання та емуляція, тестування на проникнення, аналіз мережевого трафіку.

Завдання дослідження

1. Проаналізувати стан кібербезпеки та класифікувати мережеві атаки
2. Порівняти існуючі рішення у сфері кіберполігонів
3. Визначити архітектурні вимоги до кіберполігону
4. Спроектувати та реалізувати кіберполігон на базі віртуалізації
5. Розробити й апробувати сценарії мережевих атак
6. Інтегрувати засоби моніторингу (IDS/SIEM) та оцінити їх ефективність
7. Провести апробацію та сформулювати рекомендації

РОЗДІЛ

1

Аналіз предметної галузі та постановка задачі

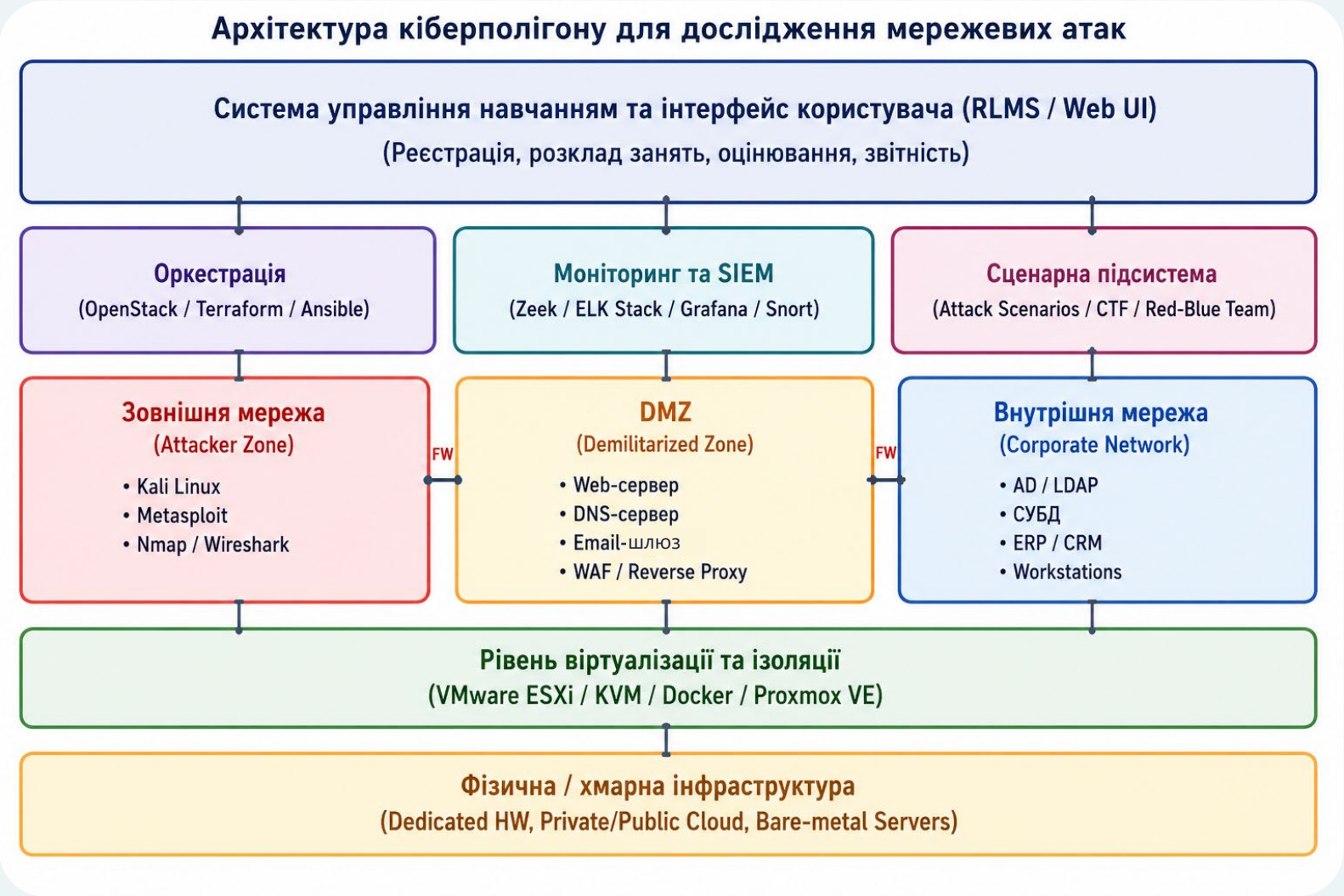
Сучасний стан, класифікація атак, огляд рішень

Мережеві атаки на корпоративну інфраструктуру

КАТЕГОРІЯ АТАКИ	ПРИКЛАДИ ТЕХНІК	РІВЕНЬ OSI	ЦІЛЬ
DoS / DDoS	SYN/UDP/HTTP Flood, Amplification	L3–L7	Недоступність сервісу
Мережеві атаки	ARP/IP Spoofing, ICMP Redirect	L2–L3	Перехоплення трафіку
MITM	SSL Stripping, DNS Spoofing	L3–L7	Перехоплення даних
Атаки на застосунки	SQL Injection, XSS, CSRF	L7	Дані / виконання коду
Атаки на автентифікацію	Brute Force, Pass-the-Hash, Kerberoasting	L4–L7	Несанкц. доступ
APT / Lateral Movement	SMB Relay, WMI Exec, PsExec	L4–L7	Поширення в мережі
Шкідливе ПЗ	Ransomware, Trojan, Rootkit, C2	L3–L7	Шифрування / контроль

Кіберполігон забезпечує дослідження щонайменше **5 із 7** категорій атак, релевантних для корпоративного середовища.

Архітектура та компоненти кіберполігону



6 КЛЮЧОВИХ РІВНІВ

Інтерфейс / RLMS
реєстрація, сценарії, звітність

Оркестрація
Terraform, Ansible, OpenStack

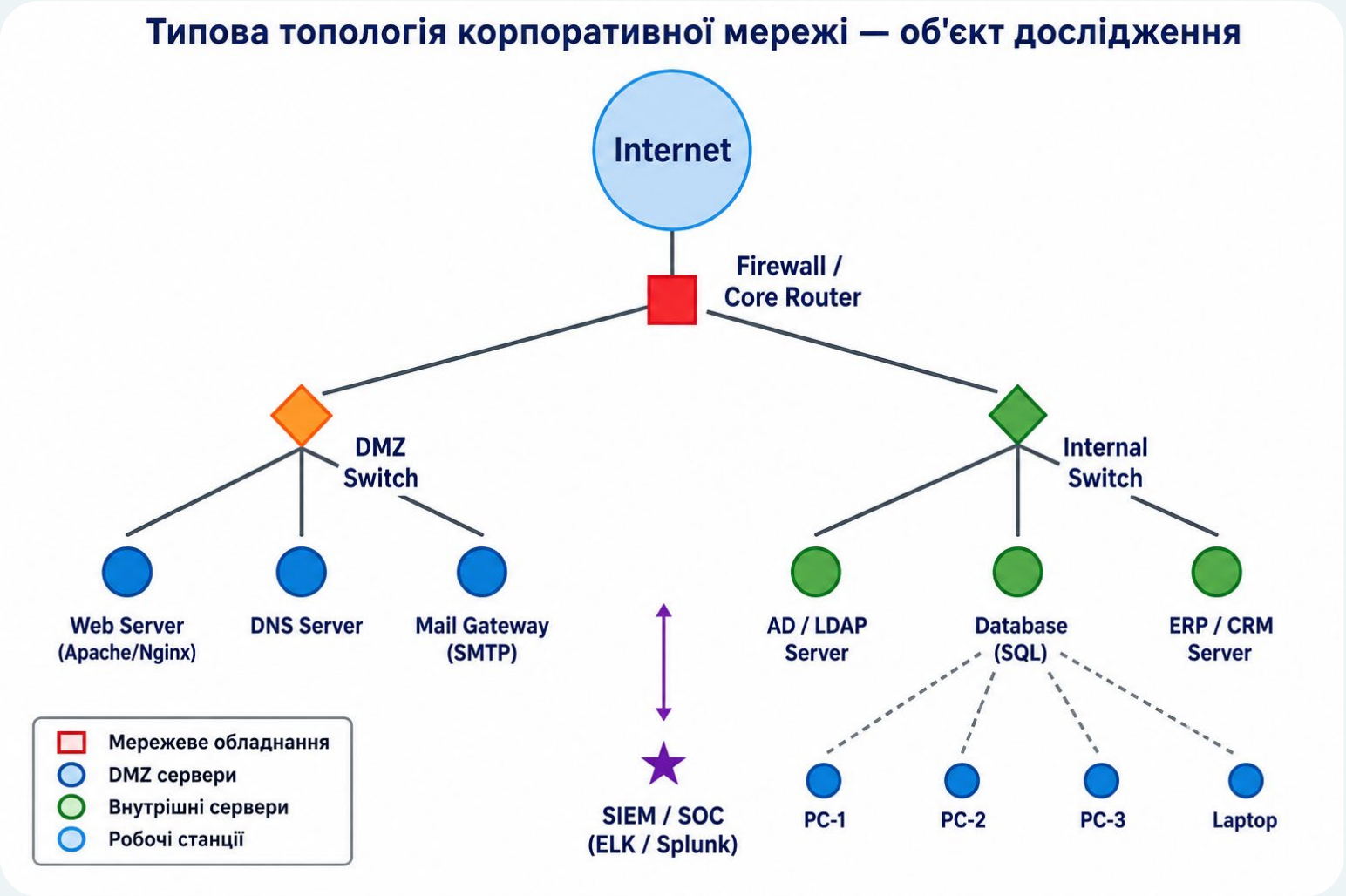
Моніторинг / SIEM
Suricata, Elastic Stack, Grafana

Цільова інфраструктура
3 зони: External • DMZ • Internal

Віртуалізація / ізоляція
KVM • Docker • Proxmox VE

Фізична / хмарна основа
сервери, приватна/публічна хмара

Топологія корпоративної мережі



Зовнішня мережа

вузол зловмисника (Attacker Zone)

DMZ

Web · DNS · Mail — публічні сервіси

Внутрішня мережа

AD/LDAP · СУБД · ERP · робочі станції

SIEM / SOC

наскрізний збір телеметрії з усіх зон

Порівняльний аналіз кіберполігонів

Жодне відкрите рішення не задовольняє всіх вимог сучасного середовища

NCR, Cyberbit, IBM

найвища реалістичність, але висока вартість і закритий код

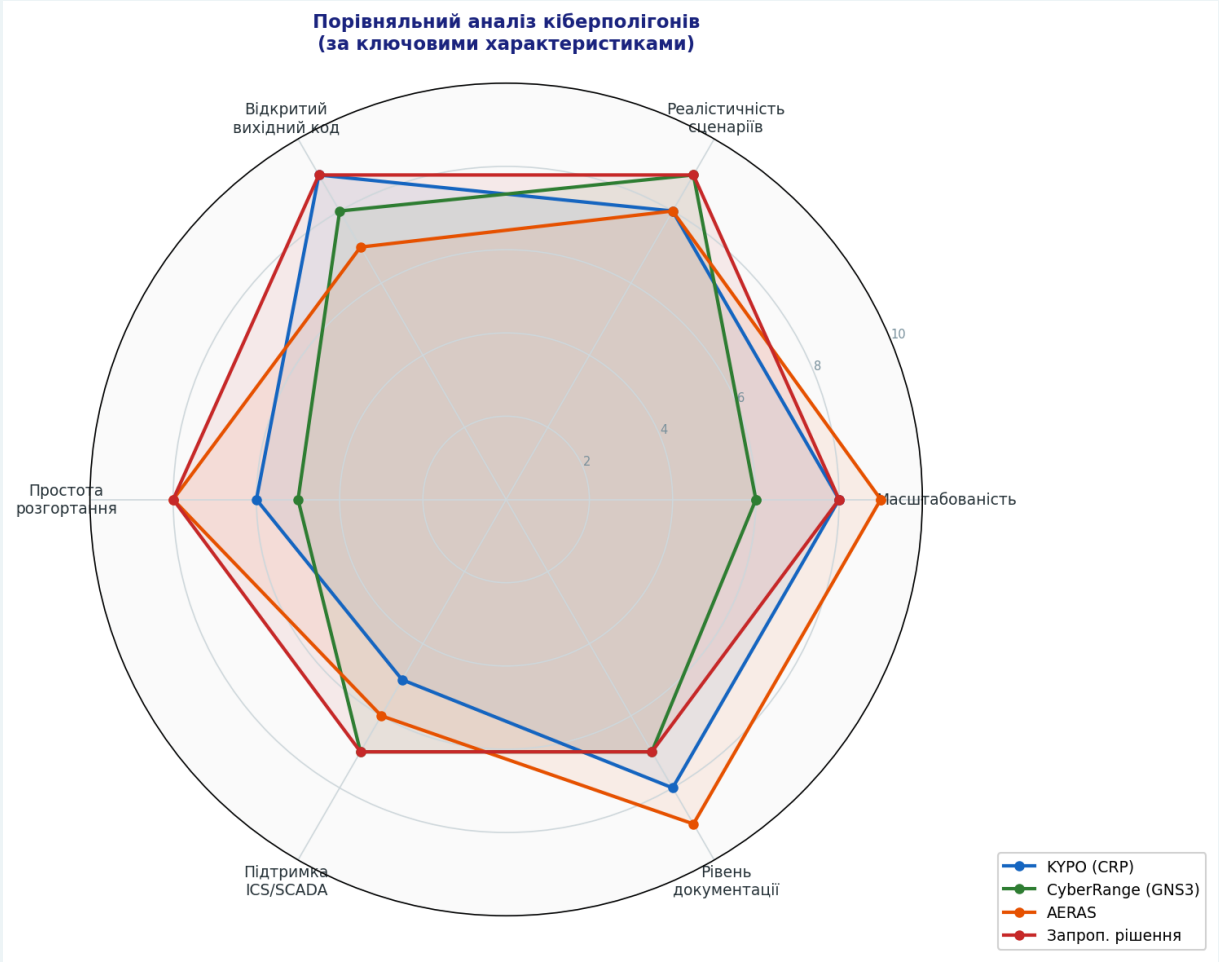
KYPO CRP

зрілий Open Source, але потребує важкого OpenStack

GNS3 / EVE-NG

гнучке моделювання мережі без інтегрованого SIEM

ВИСНОВОК: доцільно розробити власне рішення на базі відкритого ПЗ



Вимоги до кіберполігону

ФУНКЦІОНАЛЬНІ (Ф1–Ф5)

Ф1	Трирівнева топологія з реалістичними сервісами
Ф2	Підтримка ≥ 5 категорій мережевих атак
Ф3	Інтеграція IDS/SIEM з кореляцією подій
Ф4	Автоматизоване розгортання (IaC)
Ф5	Документування та відтворюваність сценаріїв

НЕФУНКЦІОНАЛЬНІ (НФ1–НФ5)

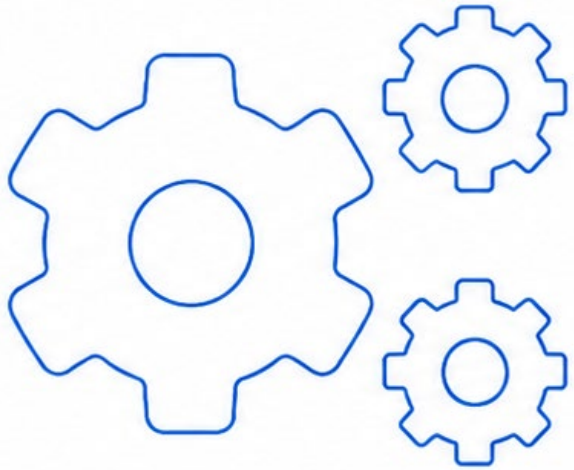
НФ1	Ресурсна ефективність (сервер середньої потужності)
НФ2	Масштабованість архітектури
НФ3	Відкритість — лише Open Source
НФ4	Безпека: повна мережева ізоляція
НФ5	Достатній рівень технічної документації

РОЗДІЛ 2

2

Обґрунтування та розроблення рішення

Технології, архітектура, сценарії атак



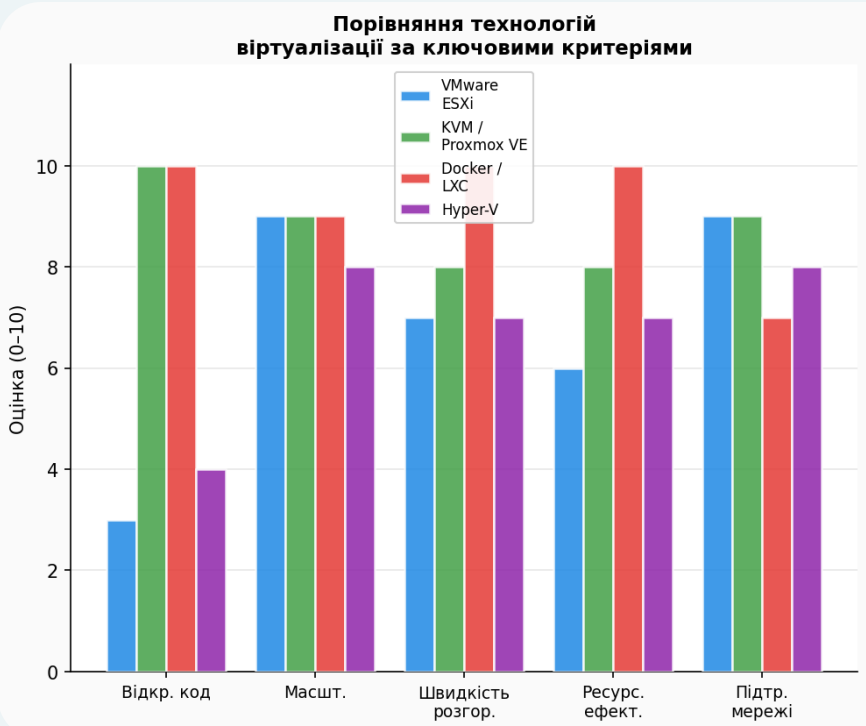
Програмний стек кіберполігону

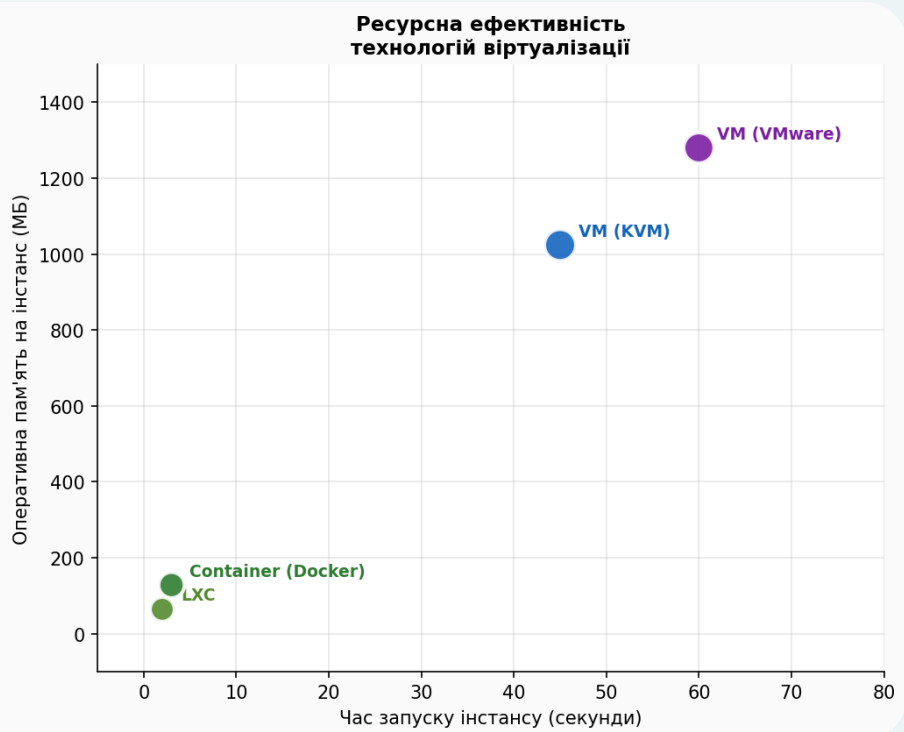
Атакуючий	Kali Linux 2024.2 · Metasploit · Nmap · Hydra · hping3
Мережа	pfSense 2.7 · VLAN 802.1Q · NAT · OpenVPN
Сервіси	Ubuntu 22.04 · Win Server 2022 · Apache+DVWA · MySQL · Samba AD
IDS / SIEM	Suricata 7.x · Elastic Stack 8.x (ELK)
Оркестрація	Proxmox VE 8.x · Terraform · Ansible · Docker

Обґрунтування платформи віртуалізації

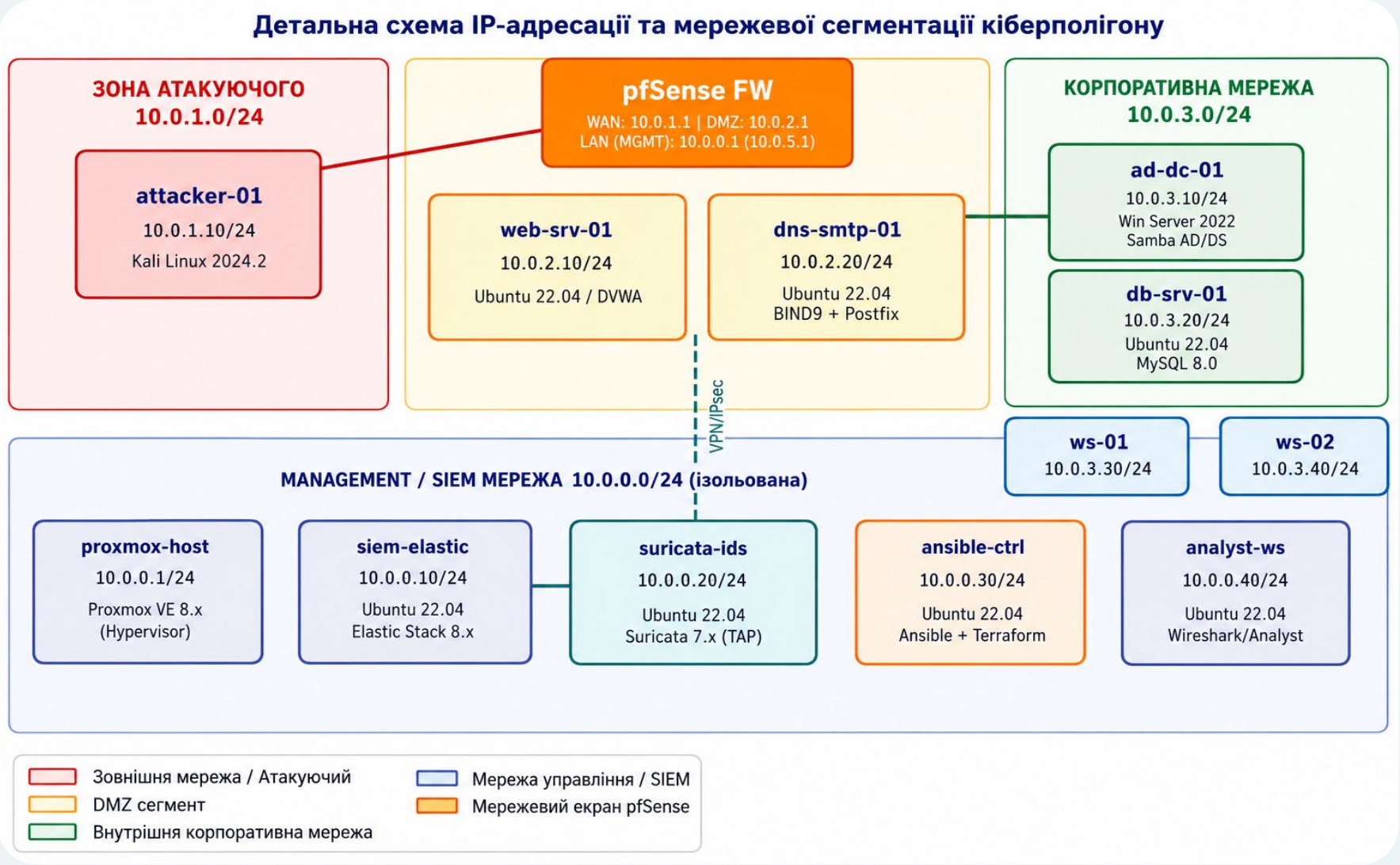
Обрано Proxmox VE 8.x

- Повністю відкритий код (GNU GPL/AGPL)
- KVM-ВМ + LXC-контейнери в одній платформі
- Інтегрований web-інтерфейс, ZFS, snapshots
- Офіційний Terraform-провайдер для IaC
- Docker Compose — для мікросервісів SIEM





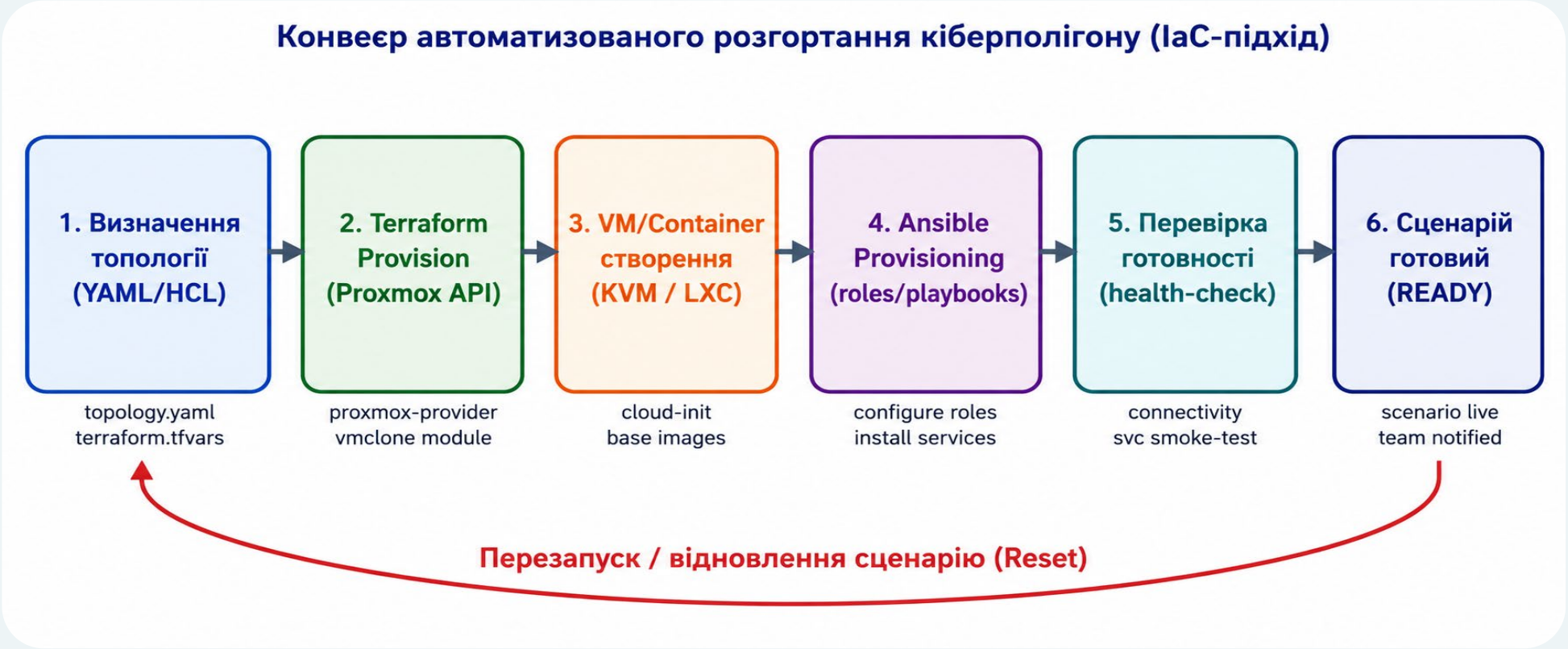
Мережева архітектура та IP-адресація



4 ізольовані зони

- **Attacker** — 10.0.1.0/24
- **DMZ** — 10.0.2.0/24
- **LAN** — 10.0.3.0/24
- **Management** — 10.0.0.0/24

Конвеєр розгортання (Infrastructure-as-Code)



Terraform

декларативне створення ВМ через Proxmox API

Ansible

конфігурування вузлів за ролями (playbooks)

5–10 хв

повне відтворюване розгортання середовища

Матриця сценаріїв атак (MITRE ATT&CK)

Матриця сценаріїв атак кіберполігону (MITRE ATT&CK alignment)

Сценарій атаки	Тактика MITRE	Цільовий вузол	Інструмент атакуючого	IDS-виявлення	Складність
DDoS (SYN/UDP/HTTP Flood)	TA0040 Impact (T1498)	web-srv-01 DMZ	hping3 Scapy	Так (Suricata)	●●○○○
ARP Spoofing / MITM	TA0006 Credential Access (T1557)	web-srv-01 ws-01	arpspoof Bettercap	Так (Suricata)	●●●○○
SQL Injection (DVWA)	TA0009 Collection (T1190)	web-srv-01 MySQL	SQLmap Burp Suite	Так (ModSec)	●●○○○
Brute Force / Credential	TA0006 Cred.Access (T1110)	ad-dc-01 SSH-сервери	Hydra Medusa	Так (Suricata)	●●●○○
Lateral Movement (PTH)	TA0008 Lateral Mov. (T1550)	ad-dc-01 db-srv-01	Impacket PsExec	Частково (ELK)	●●●●○
Ransomware Simulation	TA0040 Impact (T1486)	ws-01, ws-02 db-srv-01	Custom script + OpenSSL	Так (Wazuh)	●●●●●

● = рівень складності (1–5)

6 сценаріїв

DDoS
SYN/UDP/HTTP Flood

MITM
ARP Spoofing

SQL Injection
через DVWA

Brute Force
SSH / AD

Lateral Movement
Pass-the-Hash

Ransomware
симуляція шифрування

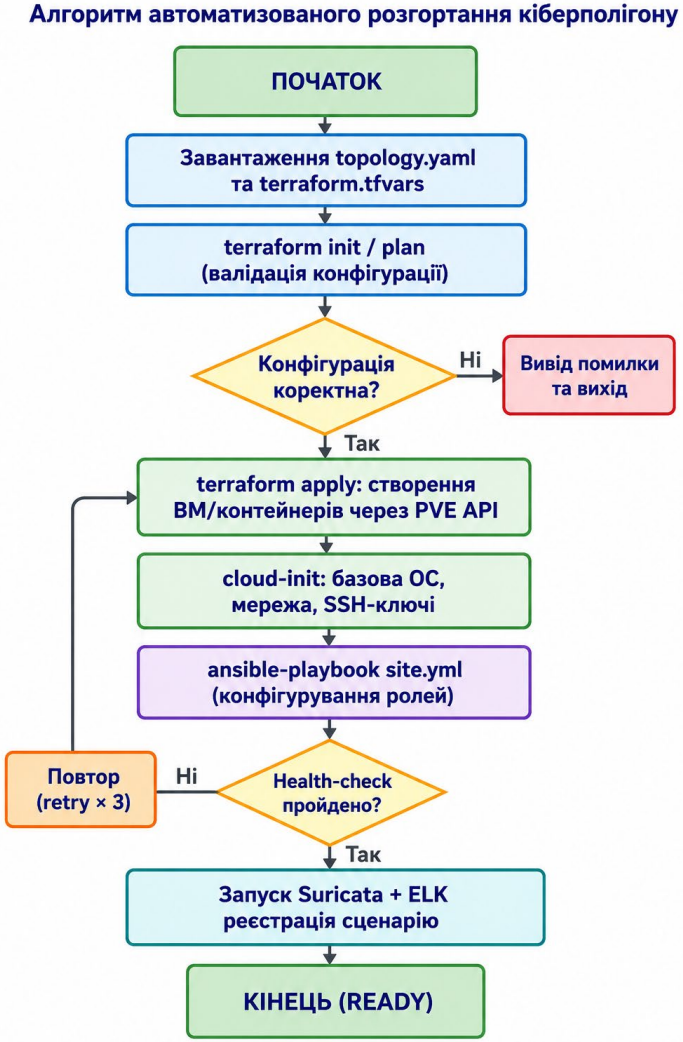
РОЗДІЛ

3

РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ

Скрипти, експерименти, оцінка ефективності

Автоматизація та готовий інструментарій



ddos_syn_flood.sh

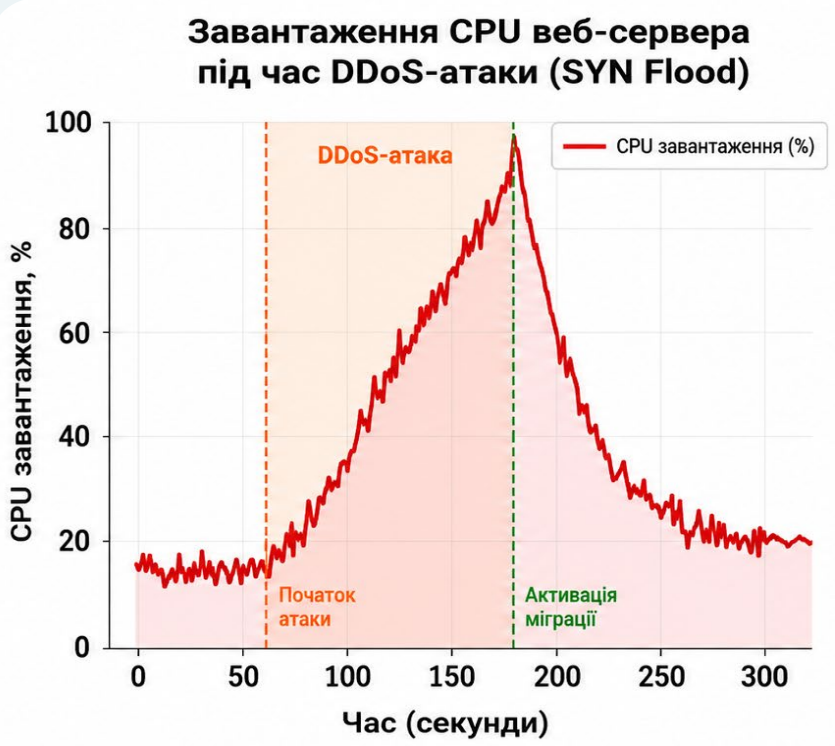
```
#!/bin/bash
TARGET="10.0.2.10"; PORT=80; DURATION=${1:-120}
timeout "$DURATION" hping3 -S --flood \
      --rand-source -p $PORT $TARGET
curl -s -o /dev/null -w "HTTP %{http_code}" $TARGET
```

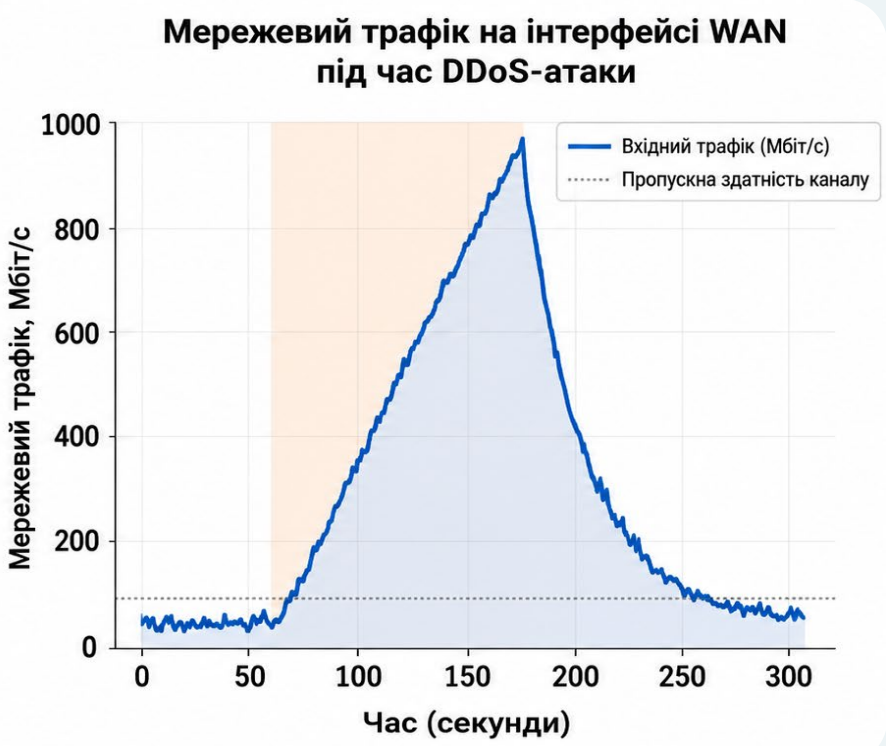
16 робочих лістингів — Terraform, Ansible, Docker Compose, Suricata, скрипти атак

Повна автоматизація — розгортання → конфігурування → перевірка → reset

Власні правила Suricata — local.rules для 6 сценаріїв атак

Поведінка під час DDoS-атаки





Завантаження CPU та мережевий трафік під час SYN Flood (120 с)

15% – 85%

зростання CPU під час атаки

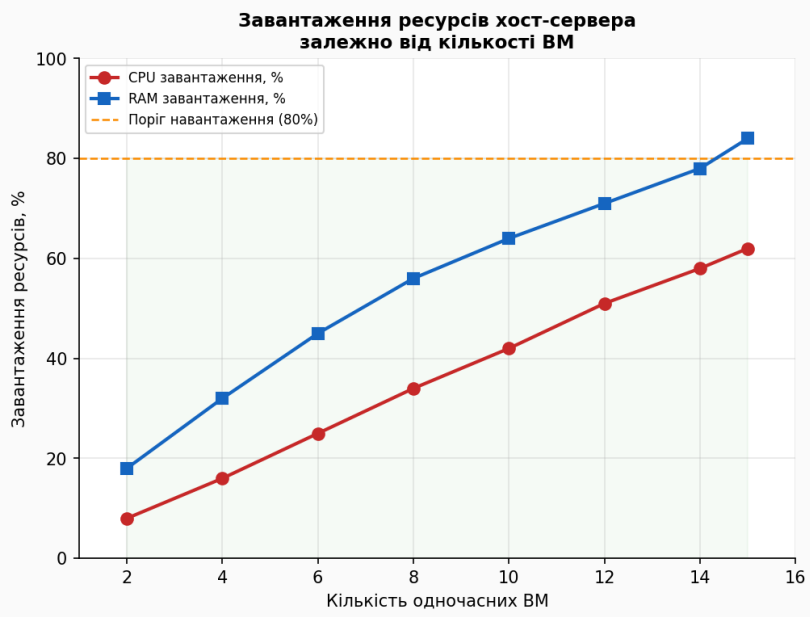
~920 Мбіт/с

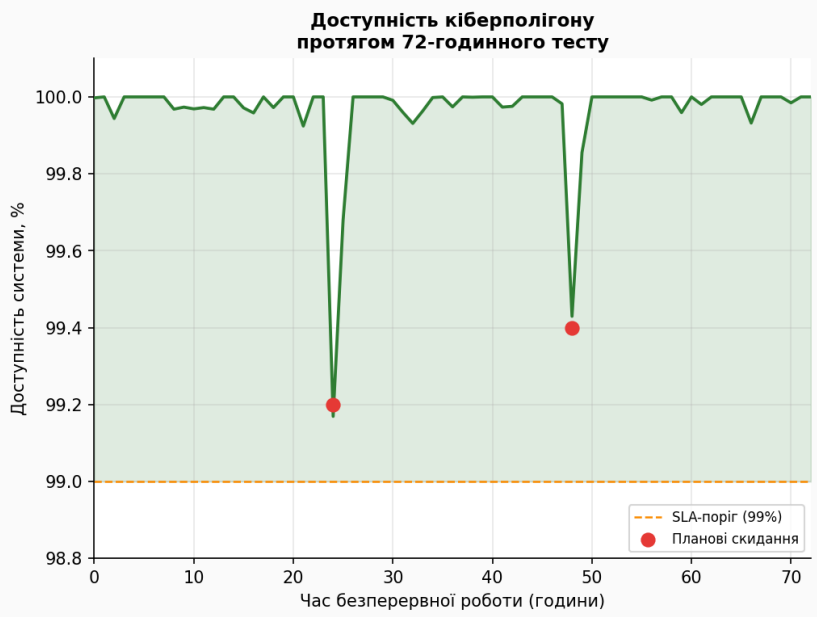
пікове значення трафіку (вхідний потік)

30–40 с

відновлення після активації мітигації

Масштабованість і надійність





62% / 84%

CPU / RAM при 15 одночасних ВМ

99,86%

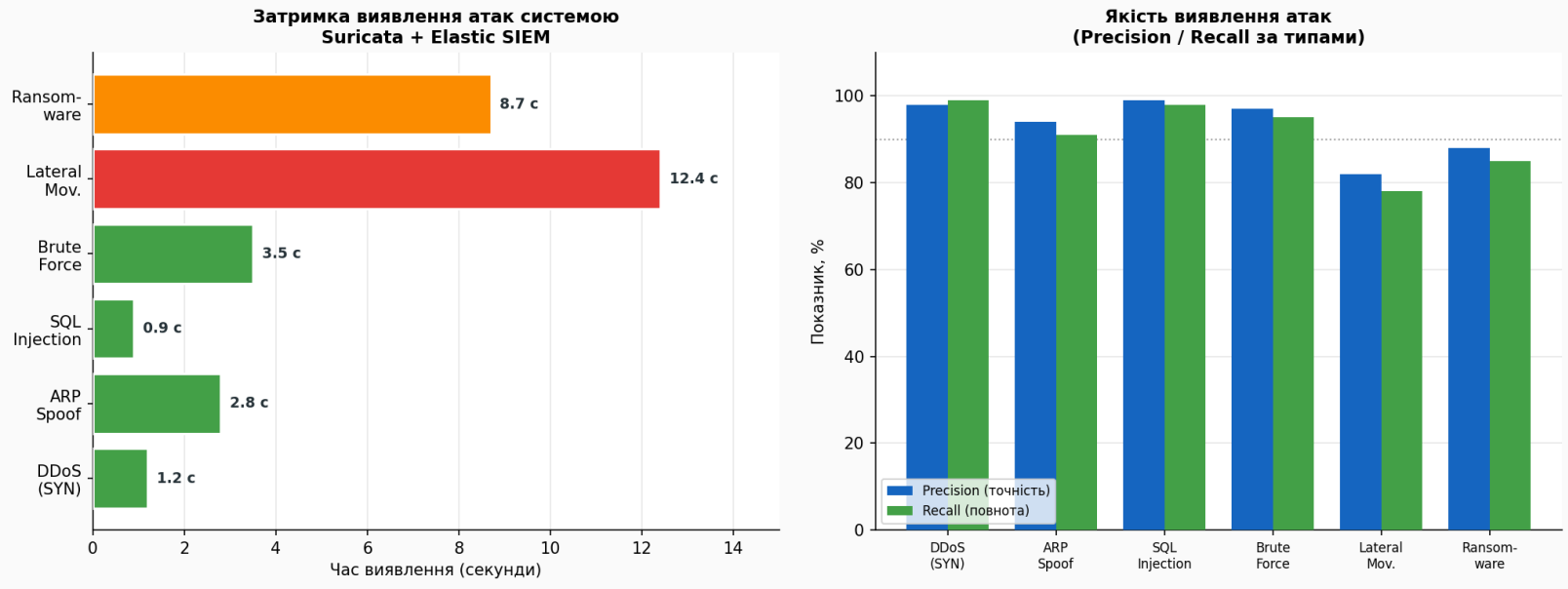
доступність системи (72-год тест)

0

незапланованих збоїв за весь період

Використовувались ресурси не більше 85% від доступних протягом 72 годин

Ефективність системи виявлення вторгнень



Затримка виявлення та якість (Precision / Recall) за типами атак

97,7%
Accuracy

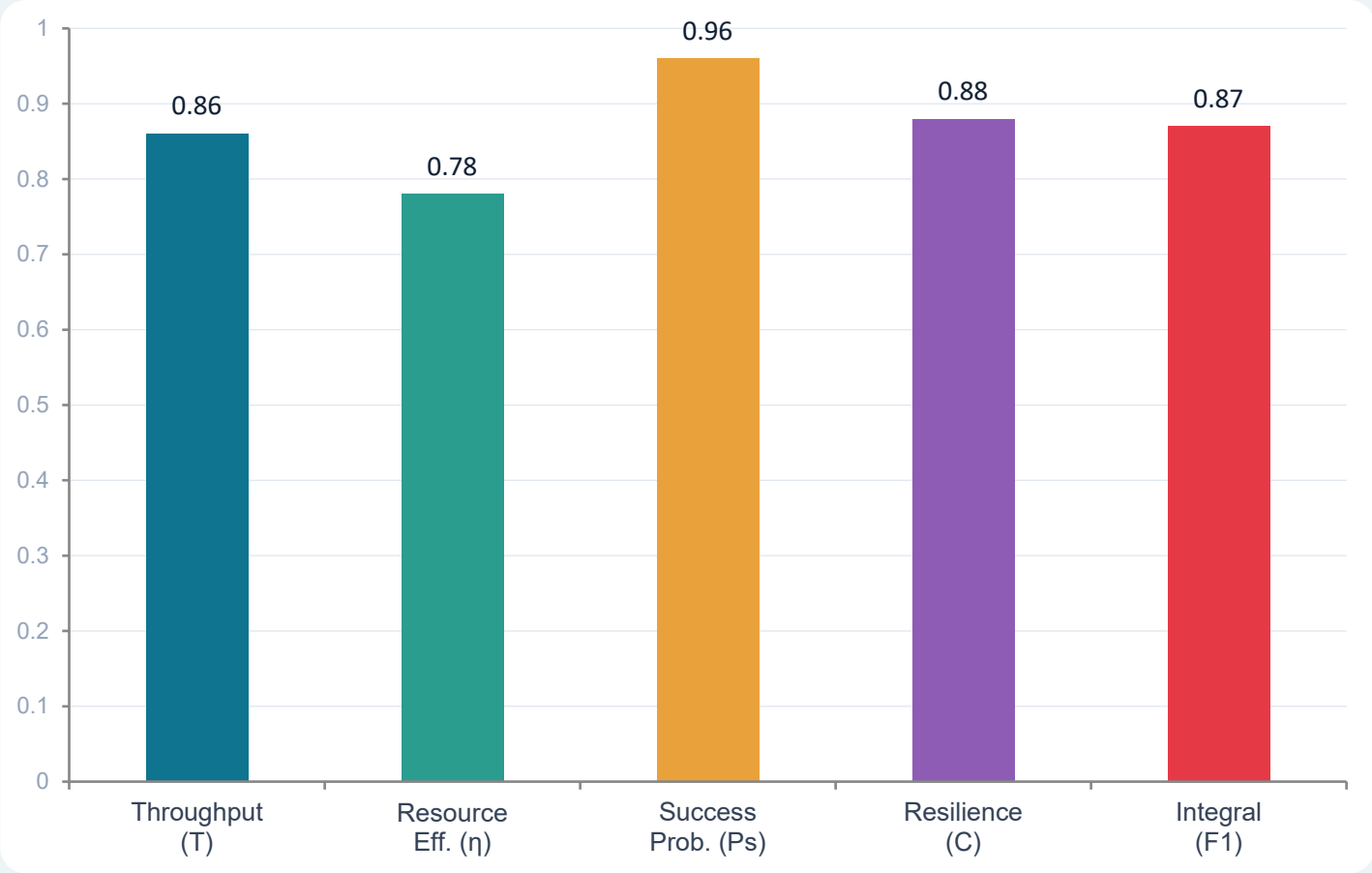
98,1%
Precision

96,5%
Recall

97,3%
F1-міра

< 3,5 с — затримка виявлення простих атак (DDoS, SQLi)

Інтегральна оцінка ефективності



Модель оцінки (Lakhno et al., 2025)

$$F1 = \alpha \cdot E + \beta \cdot S + \gamma \cdot R$$

зважена сума ефективності, надійності та стійкості (α=β=γ=0,33)

ІНТЕГРАЛЬНА ОЦІНКА

0,87

високий рівень ефективності

ПІДСУМКИ

Загальні висновки

Мету досягнуто

розроблено працездатний кіберполігон на базі відкритого ПЗ

Доступність 99,86%

стабільна робота протягом 72-год тесту

Усі вимоги виконано

Ф1–Ф5 та НФ1–НФ5 повністю задоволені

F1-міра 97,3%

висока точність виявлення атак

6 сценаріїв атак

реалізовано та виявлено системою моніторингу

Оцінка 0,87

високий інтегральний рівень ефективності

НАПРЯМИ ПОДАЛЬШОГО РОЗВИТКУ

ML-аналіз трафіку

поведінкове виявлення складних атак

HIDS-агенти Wazuh

контроль цілісності та внутрішні загрози

Сценарії ICS/SCADA

розширення на промислові системи

Кластеризація Proxmox

масштабованість і відмовостійкість

Дякую за увагу!

Готова відповісти на ваші запитання