RAPORT OPERACYJNY: blox-tak-server-vm-2026-01-20-03-11-56

---

1. METRYKA OPERACJI

Data audytu:	2026-01-24 16:00:14
Operator:	[redacted]
Cel (VM):	blox-tak-server-vm-2026-01-20-03-11-56
Adres (WAN IP):	[redacted]
Adres (LAN IP):	[redacted] (SECURE SSH)
Lokalizacja GCP:	europe-north1-a
Typ Maszyny:	e2-custom-12-49152

2. STATUS ZASOBÓW SYSTEMOWYCH

Nazwa Hosta:	takserver
System:	Ubuntu 22.04.5 LTS
Jądro:	[redacted]
Czas pracy:	up 8 minutes
Zużycie RAM:	39Gi/47Gi used
Zużycie Dysku:	22% of 146G

3. USŁUGI DOCKER I KONTENERY

NAZWA KONTENERA	STATUS	PORTY / INFO
malcolm-nginx-proxy-1	Up 5 minutes (healthy)	XXX.XXX.XXX.XXX:443->443/tcp
malcolm-dashboards-1	Up 5 minutes (healthy)	5601/tcp
malcolm-netbox-1	Up 5 minutes (healthy)	9001/tcp
malcolm-zeek-1	Up 5 minutes (healthy)	
malcolm-dashboards-helper-1	Up 5 minutes (healthy)	28991/tcp
malcolm-arkime-1	Up 5 minutes (healthy)	8000/tcp, 8005/tcp, 8081/tcp
malcolm-logstash-1	Up 5 minutes (healthy)	5044/tcp, 9001/tcp, 9600/tcp
malcolm-pcap-monitor-1	Up 5 minutes (healthy)	30441/tcp
malcolm-file-monitor-1	Up 5 minutes (healthy)	3310/tcp, 8006/tcp
malcolm-filebeat-1	Up 5 minutes (healthy)	
malcolm-zeek-live-1	Up 5 minutes (healthy)	
malcolm-api-1	Up 5 minutes (healthy)	5000/tcp
malcolm-arkime-live-1	Up 5 minutes (healthy)	
malcolm-keycloak-1	Up 5 minutes (healthy)	8080/tcp, 8443/tcp, 9000/tcp
malcolm-postgres-1	Up 5 minutes (healthy)	5432/tcp
malcolm-freq-1	Up 5 minutes (healthy)	10004/tcp
malcolm-opensearch-1	Up 5 minutes (healthy)	9200/tcp, 9300/tcp, 9600/tcp, 9650/tcp
malcolm-upload-1	Up 5 minutes (healthy)	22/tcp, 80/tcp
malcolm-redis-1	Up 5 minutes (healthy)	6379/tcp
malcolm-pcap-capture-1	Up 5 minutes (healthy)	
malcolm-redis-cache-1	Up 5 minutes (healthy)	6379/tcp
malcolm-suricata-1	Up 5 minutes (healthy)	
malcolm-htadmin-1	Up 5 minutes (healthy)	80/tcp
malcolm-suricata-live-1	Up 5 minutes (healthy)	
tak-server-tak-1	Up 8 minutes	XXX.XXX.XXX.XXX:8089->8089/tcp, [::]:8089->8089/tcp, XXX.XXX.XXX.XXX:8443-8444->8443-8444/tcp, [::]:8443-8444->8443-8444/tcp, XXX.XXX.XXX.XXX:8446->8446/tcp, [::]:8446->8446/tcp, XXX.XXX.XXX.XXX:9000-9001->9000-9001/tcp, [::]:9000-9001->9000-9001/tcp
tak-server-db-1	Up 8 minutes	5432/tcp

---

4. LOGI I ARTEFAKTY

Logi systemowe: OCZEKIWANIE (Patrz Faza 2)

[STATUS SYSTEMU: AKTYWNY I BEZPIECZNY]

ZAŁĄCZNIK A: SPIS ZAWARTOŚCI LOGÓW

Niniejszy dokument potwierdza ekstrakcję następujących logów systemowych i kontenerów.

METADANE ARCHIWUM

Nazwa Archiwum: logs_20260124_160447.tar.gz

Suma Kontrolna (MD5): d85bb5b8da5b01419c59f92fd12e4eee

NAZWA PLIKU	ROZMIAR (B)
harvest_20260124_160447/docker_internal/tak-server-tak-1/logs/takserver-messaging.2026-01-20.log.gz	2305
harvest_20260124_160447/docker_internal/tak-server-tak-1/logs/takserver-config.log	2250
harvest_20260124_160447/docker_internal/tak-server-tak-1/logs/takserver-plugins.2026-01-20.log.gz	1046
harvest_20260124_160447/docker_internal/tak-server-tak-1/logs/takserver-db-audit.log	0
harvest_20260124_160447/docker_internal/tak-server-tak-1/logs/takserver-plugins.log	8615
harvest_20260124_160447/docker_internal/tak-server-tak-1/logs/takserver-esapi.log	0
harvest_20260124_160447/docker_internal/tak-server-tak-1/logs/takserver-api.log	12370
harvest_20260124_160447/docker_internal/tak-server-tak-1/logs/takserver-messaging.log	15031
harvest_20260124_160447/docker_internal/tak-server-tak-1/logs/takserver-api.2026-01-20.log.gz	1756
harvest_20260124_160447/docker_internal/tak-server-tak-1/logs/takserver-config.2026-01-20.log.gz	26521
harvest_20260124_160447/docker_internal/tak-server-tak-1/logs/takserver-retention.log	13169
harvest_20260124_160447/docker_internal/tak-server-tak-1/logs/takserver-retention.2026-01-20.log.gz	2768
harvest_20260124_160447/docker_internal/tak-server-tak-1/logs/takserver.log	683458
harvest_20260124_160447/docker_internal/tak-server-tak-1/logs/takserver-api-access.log	0
harvest_20260124_160447/docker_std/malcolm-postgres-1.log	9911
harvest_20260124_160447/docker_std/malcolm-dashboards-1.log	26886
harvest_20260124_160447/docker_std/malcolm-htadmin-1.log	368
harvest_20260124_160447/docker_std/malcolm-file-monitor-1.log	8627
harvest_20260124_160447/docker_std/malcolm-redis-cache-1.log	3591
harvest_20260124_160447/docker_std/malcolm-arkime-1.log	49266
harvest_20260124_160447/docker_std/malcolm-suricata-1.log	2647
harvest_20260124_160447/docker_std/tak-server-tak-1.log	0
harvest_20260124_160447/docker_std/malcolm-pcap-monitor-1.log	2365
harvest_20260124_160447/docker_std/malcolm-zeek-live-1.log	2531
harvest_20260124_160447/docker_std/malcolm-arkime-live-1.log	389
harvest_20260124_160447/docker_std/tak-server-db-1.log	32846
harvest_20260124_160447/docker_std/malcolm-suricata-live-1.log	2871
harvest_20260124_160447/docker_std/malcolm-dashboards-helper-1.log	63761
harvest_20260124_160447/docker_std/malcolm-freq-1.log	558
harvest_20260124_160447/docker_std/malcolm-keycloak-1.log	320
harvest_20260124_160447/docker_std/malcolm-filebeat-1.log	123932
harvest_20260124_160447/docker_std/malcolm-logstash-1.log	181011
harvest_20260124_160447/docker_std/malcolm-upload-1.log	4302
harvest_20260124_160447/docker_std/malcolm-nginx-proxy-1.log	244654
harvest_20260124_160447/docker_std/malcolm-pcap-capture-1.log	841
harvest_20260124_160447/docker_std/malcolm-zeek-1.log	1032
harvest_20260124_160447/docker_std/malcolm-redis-1.log	7415
harvest_20260124_160447/docker_std/malcolm-opensearch-1.log	306725

ZAŁĄCZNIK A: SPIS ZAWARTOŚCI LOGÓW

harvest_20260124_160447/docker_std/malcolm-netbox-1.log	2443271
harvest_20260124_160447/docker_std/malcolm-api-1.log	882
harvest_20260124_160447/system/dmesg_boot.txt	50491
harvest_20260124_160447/system/syslog	1806957
harvest_20260124_160447/system/auth.log	374186

[WERSJA PUBLICZNA: TYLKO METADANE - TREŚĆ ZABEZPIECZONA]

KLAUZULA PRAWNA / POLITYKA RETENCJI

Powyższy wykaz stanowi potwierdzenie zabezpieczenia materiału dowodowego. Pełny pakiet logów (.tar.gz) zawiera dane wrażliwe i jest przechowywany w bezpiecznym depozycie offline. Może zostać udostępniony odpowiednim organom wyłącznie w uzasadnionych przypadkach.

ZAŁĄCZNIK B: BEZPIECZEŃSTWO I SIECI

1. PUNKT PRZYWRACANIA (ZIMNA MIGAWKA)

System zatrzymany. Gwarantowana spójność systemu plików.

ID Snapshotu: snap-tak-cold-20260124-161022

Data utworzenia: 2026-01-24 16:11:36 (Local)

Rozmiar (Snap/Dysk): 19.52 GB (Real) / 150 GB (Disk)

Status: READY

ŹRÓDŁO OBRAZU (URI - DISK_IMAGE):

https://www.googleapis.com/compute/v1/projects/blox-tak-server/global/snapshots/snap-tak-cold-20260124-161022

2. PRZECHWYCONY RUCH SIECIOWY (PCAPNG)

ŹRÓDŁO	NAZWA PLIKU	ROZMIAR
mdc2	2026-01-24_11-36-48_enp3s0.pcapng	778.74 MB
mdc2	2026-01-24_04-46-55_enp3s0.pcapng	95.97 MB
mdc2	2026-01-24_14-24-41_enp3s0.pcapng	345.91 MB
VM1	2026-01-24_04-47-34_wg0.pcapng	28.08 MB
VM1	2026-01-24_15-52-45_ens4.pcapng	7.43 MB
VM1	2026-01-24_03-22-49_wg0.pcapng	67.41 MB
VM1	2026-01-24_03-22-33_ens4.pcapng	699.21 MB
VM1	2026-01-24_04-47-16_ens4.pcapng	27.68 MB
VM1	2026-01-24_15-53-08_wg0.pcapng	31.01 MB

OSTRZEŻENIE PRAWNE (SIGINT/COMINT)

Pliki PCAPNG zawierają pełny zrzut pakietów sieciowych. Pliki te są sklasyfikowane jako WRAŻLIWE. Przechowywane są w odseparowanym depozycie i NIE są dołączane do treści raportu (Powyższa lista służy jako dowód zabezpieczenia).

EVIDENCE PACKAGE STRUCTURE / STRUKTURA PAKIETU DOWODOWEGO

```
EVIDENCE_VM1_blox-tak-server-vm-2026-01-20-03-11-56_20260124_1615
|-- NETWORK_PCAP
|   |-- mdc2
|   |   |-- 2026-01-24_04-46-55_enp3s0.pcapng
|   |   |-- 2026-01-24_11-36-48_enp3s0.pcapng
|   |   `-- 2026-01-24_14-24-41_enp3s0.pcapng
|   `-- VM1
|       |-- 2026-01-24_03-22-33_ens4.pcapng
|       |-- 2026-01-24_03-22-49_wg0.pcapng
|       |-- 2026-01-24_04-47-16_ens4.pcapng
|       |-- 2026-01-24_04-47-34_wg0.pcapng
|       |-- 2026-01-24_15-52-45_ens4.pcapng
|       `-- 2026-01-24_15-53-08_wg0.pcapng
|-- REPORTS
|   |-- RAPORT_blox-tak-server-vm-2026-01-20-03-11-56_20260124_1600_PL.pdf
|   |-- RAPORT_blox-tak-server-vm-2026-01-20-03-11-56_20260124_1600_PL_PUBLICZNY.pdf
|   |-- REPORT_blox-tak-server-vm-2026-01-20-03-11-56_20260124_1600_EN.pdf
|   `-- REPORT_blox-tak-server-vm-2026-01-20-03-11-56_20260124_1600_EN_PUBLIC.pdf
|-- SNAPSHOT_INFO.txt
`-- SYSTEM_LOGS
    |-- logs_20260124_160447
    |   `-- harvest_20260124_160447
    |       |-- docker_internal
    |       |   `-- tak-server-tak-1
    |       |       `-- logs
    |       |           |-- takserver-api.2026-01-20.log.gz
    |       |           |-- takserver-api-access.log
    |       |           |-- takserver-api.log
    |       |           |-- takserver-config.2026-01-20.log.gz
    |       |           |-- takserver-config.log
    |       |           |-- takserver-db-audit.log
    |       |           |-- takserver-esapi.log
    |       |           |-- takserver.log
    |       |           |-- takserver-messaging.2026-01-20.log.gz
    |       |           |-- takserver-messaging.log
    |       |           |-- takserver-plugins.2026-01-20.log.gz
    |       |           |-- takserver-plugins.log
    |       |           |-- takserver-retention.2026-01-20.log.gz
    |       |           `-- takserver-retention.log
    |       |-- docker_std
    |       |   |-- malcolm-api-1.log
    |       |   |-- malcolm-arkime-1.log
    |       |   |-- malcolm-arkime-live-1.log
    |       |   |-- malcolm-dashboards-1.log
    |       |   |-- malcolm-dashboards-helper-1.log
    |       |   |-- malcolm-filebeat-1.log
    |       |   |-- malcolm-file-monitor-1.log
    |       |   |-- malcolm-freq-1.log
```

EVIDENCE PACKAGE STRUCTURE / STRUKTURA PAKIETU DOWODOWEGO

```
    |       |   |-- malcolm-htadmin-1.log
    |       |   |-- malcolm-keycloak-1.log
    |       |   |-- malcolm-logstash-1.log
    |       |   |-- malcolm-netbox-1.log
    |       |   |-- malcolm-nginx-proxy-1.log
    |       |   |-- malcolm-opensearch-1.log
    |       |   |-- malcolm-pcap-capture-1.log
    |       |   |-- malcolm-pcap-monitor-1.log
    |       |   |-- malcolm-postgres-1.log
    |       |   |-- malcolm-redis-1.log
    |       |   |-- malcolm-redis-cache-1.log
    |       |   |-- malcolm-suricata-1.log
    |       |   |-- malcolm-suricata-live-1.log
    |       |   |-- malcolm-upload-1.log
    |       |   |-- malcolm-zeek-1.log
    |       |   |-- malcolm-zeek-live-1.log
    |       |   |-- tak-server-db-1.log
    |       |   `-- tak-server-tak-1.log
    |       `-- system
    |           |-- auth.log
    |           |-- dmesg_boot.txt
    |           `-- syslog
    `-- logs_20260124_160447.tar.gz

12 directories, 58 files
```

Gmail Łukasz Andruszkiewicz <luke.strider.gm@gmail.com>

BLOX-TAK-SERVER-IPPU-GCP

1 message

luke.strider.gm@gmail.com <luke.strider.gm@gmail.com> Mon, Jan 19, 2026 at 3:36 AM
To: luke.strider.gm@gmail.com

Witaj, LukeStriderGm-PL!

Dziękuję za Twoją rejestrację w dniu **2026-01-18 04:09:00**. Poniżej znajdują się linki do Twojego zgłoszenia:

- Link do Formularza
- Wpis w Arkuszu Google

W załączeniu przesyłam paczkę **ZIP**, którą należy zaimportować w aplikacji **ATAK**. Paczka wymaga również ręcznego rozpakowania, gdyż znajduje się tam certyfikat **mumble.cer** dla wtyczki **VOICE** dla komunikacji głosowej VoIP. Certyfikat należy zainstalować bezpośrednio w ustawieniach systemu **ANDROID**. Hasło do serwera **MUMBLE** to: `nSkMeh5n3v84X6jn`. Adres IP hosta **MUMBLE** jest identyczny jak adres IP **Serwera-TAK** - który należy skopiować z **Preferencji Sieciowych** po imporcie paczki "Użytkownika Urządzenia Końcowego" (EUD) w aplikacji **ATAK**.

Aby uruchomić połączenie **VPN**, zainstaluj aplikację **WireGuard** na telefonie, a następnie dodaj tunel, skanując poniższy kod QR.

BLOX-TAK - SOLUTIONS FORGE

"BLOX - BLUE LIQUID OXYGEN"

"BLOX": Technical Social Organization For Creating Useful Social Solutions

Łukasz Andruszkiewicz
Ul. Żołnierska 72/6
58-562 Podgórzyn
Dolnośląskie, Poland
NIP: PL 6112444076

Tel: +48 571 920 898
E-mail: luke.strider.gm@gmail.com
GitHub: LukeStriderGM
LinkedIn: LukeBlueLOx **WWW:** BLOX-TAK-SF

IN CHAOS QUAERO GRAAL

✌️♻️🌌🚀🌎🌍🌏🛰️🌌♻️✌️

IUCP-IPPU_PACKAGE_LukeStriderGm-PL.zip
10K

BLOX Logo

Instrukcja dla Admina (Ubuntu 22.04)

Ten pakiet zawiera wszystko, czego potrzebujesz, aby uzyskać pełny administracyjny dostęp do serwera TAK.

Krok 1: Konfiguracja VPN (WireGuard)

1. UWAGA! - Wymaga Się Otwartego Portu: "51820" Na "Firewall-ach".

2. Zainstaluj narzędzia WireGuard:

```
sudo apt-get update && sudo apt-get install wireguard-tools
```

3. Przenieś plik konfiguracyjny do folderu systemowego:

```
sudo mv "wg-admin-vm1.conf" "/etc/wireguard/"
```

4. Zarządzaj połączeniem VPN:

```
# Włącz:
sudo wg-quick up wg-admin-vm1

# Wyłącz:
sudo wg-quick down wg-admin-vm1
```

Krok 2: Dostęp do Paneli Webowych

1. W przeglądarce przejdź do "Ustawienia" -> "Prywatność i bezpieczeństwo" -> "Certyfikaty".
2. Wybierz "Twoje certyfikaty" i kliknij "Importuj...".
3. Wskaż plik **admin_VM1.p12**. Hasło to: **atakatak**.

Krok 3: Instalacja Klienta Mumble

1. Zaktualizuj listę pakietów w terminalu:

```
sudo apt update
```

2. Zainstaluj klienta Mumble:

```
sudo apt install mumble
```

3. Uruchom Mumble z menu aplikacji lub wpisując w terminalu komendę `mumble`.

Krok 4: Konfiguracja Klienta Mumble

1. W kliencie Mumble wybierz "Konfiguracja" -> "Certyfikaty" i zaimportuj plik **mumble-client_VM1.p12**, używając **hasła certyfikatu** podanego poniżej.
2. Dodaj nowy serwer, wpisując adres IP i port (domyślnie 64738).
3. Połącz się z serwerem. Przy pierwszym połączeniu użyj nazwy użytkownika **SuperUser** i **hasła serwera** podanego poniżej.
4. Po zalogowaniu jako SuperUser, możesz zarejestrować swoją normalną nazwę użytkownika na serwerze.

Ważne Adresy i Hasła (dostępne przez VPN)

Adres Web: `https://10.166.0.7:8443`

Serwer Mumble: `10.166.0.7`

HASŁO SERWERA (dla ATAK i logowania SuperUser w Mumble):
`nSkMeh5n3v84X6jn`

Hasło Certyfikatu Mumble (.p12, do importu): `TezSOBaQyYJNDOpe`

Login Admina TAK: `admin`

Hasło Admina TAK: `hZZxKwTXvNCMeh1!`

Hasło PostgreSQL: `WcGRERz1JMBMeh1!`