OPERATIONAL REPORT: blox-tak-server-vm-2026-01-20-03-11-56

1. OPERATION METRICS

Audit Date:	2026-01-24 16:00:13
Operator:	[redacted]
Target (VM):	blox-tak-server-vm-2026-01-20-03-11-56
Host (WAN IP):	[redacted]
Host (LAN IP):	[redacted] (SECURE SSH)
GCP Location:	europe-north1-a
Machine Type:	e2-custom-12-49152

2. SYSTEM HEALTH & RESOURCES

Hostname:	takserver
System:	Ubuntu 22.04.5 LTS
Kernel:	[redacted]
Uptime:	up 8 minutes
RAM Usage:	39Gi/47Gi used
Disk Usage:	22% of 146G

3. DOCKER SERVICES & CONTAINERS

CONTAINER NAME	STATUS	PORTS / 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

OPERATIONAL REPORT: blox-tak-server-vm-2026-01-20-03-11-56

---

4. LOGS & ARTIFACTS

Logs collected: PENDING (See Phase 2)

[SYSTEM STATUS: ONLINE & SECURE]

APPENDIX A: LOG PACKAGE MANIFEST

This document certifies the extraction of the following system and container logs.

ARCHIVE METADATA

Archive Name: logs_20260124_160447.tar.gz

Integrity Check (MD5): d85bb5b8da5b01419c59f92fd12e4eee

FILENAME	SIZE (Bytes)
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

APPENDIX A: LOG PACKAGE MANIFEST

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

[PUBLIC RELEASE: METADATA ONLY - CONTENT SECURED OFFLINE]

LEGAL DISCLAIMER / DATA RETENTION POLICY

The list above confirms the security of the forensic material. The full log package (.tar.gz) contains sensitive data and is stored in a secure offline repository. It may be released to appropriate authorities, institutions, or the client only in justified cases.

APPENDIX B: INFRASTRUCTURE & NETWORK SECURITY

1. GOLDEN IMAGE CHECKPOINT (COLD STORAGE)

System stopped. Filesystem consistency guaranteed.

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

Creation Time: 2026-01-24 16:11:36 (Local)

Storage / Disk: 19.52 GB (Real) / 150 GB (Disk)

Status: READY

GOLDEN IMAGE SOURCE (URI):

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

2. NETWORK TRAFFIC INTERCEPTION (PCAPNG)

SOURCE	FILENAME	SIZE
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

LEGAL WARNING (SIGINT/COMINT)

PCAPNG files contain full network packet captures. These files are classified as HIGHLY SENSITIVE. They are stored in a separate air-gapped evidence locker and are NOT included in the standard report body (Metadata listing above serves as proof of capture).

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-IUCP-GCP

1 message

luke.strider.gm@gmail.com <luke.strider.gm@gmail.com> Mon, Jan 19, 2026 at 3:40 AM
To: luke.strider.gm@gmail.com

Hello, LukeStriderGm-EN!

Thank you for your registration on **2026-01-18 04:11:00**. Below are the links to your submission:

- Link to the Form

In the attachment, I am sending a **ZIP** package, which should be imported into the **ATAK** application. The package also requires manual unpacking, as it contains the **mumble.cer** certificate for the **VOICE** plugin for VoIP voice communication. The certificate must be installed directly in the **ANDROID** system settings. The password for the **MUMBLE** server is: `nSkMeh5n3v84X6jn`. The IP address of the **MUMBLE** host is identical to the IP address of the **TAK-Server** - which should be copied from the **Network Preferences** after importing the "End User Device" (EUD) package in **ATAK** app.

To enable a **VPN** connection, please install the **WireGuard** application on your phone and then add the tunnel by scanning the QR code below.

BLOX-TAK - SOLUTIONS FORGE

"BLOX - BLUE LIQUID OXYGEN"

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

Łukasz Andruszkiewicz
Zolnierska 72/6
58-562 Podgorzyn
Lower Silesian, Poland
VAT ID: PL 6112444076

Phone: +48 571 920 898
E-mail: luke.strider.gm@gmail.com
GitHub: LukeStriderGM
LinkedIn: LukeBlueLOx

IN CHAOS QUAERO GRAAL

✌️♻️🌌🚀🌎🌍🌏🛰️🌌♻️✌️

IUCP-IPPU_PACKAGE_LukeStriderGm-EN.zip
10K

BLOX Logo

Admin Instruction Manual (Ubuntu 22.04)

This package contains everything you need to gain full administrative access to the TAK server.

Step 1: VPN Configuration (WireGuard)

1. NOTE! - Requires Port "51820" to be Open on Firewalls.

2. Install WireGuard tools:

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

3. Move the configuration file to the system folder:

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

4. Manage the VPN connection:

```
# To turn ON:
sudo wg-quick up wg-admin-vm1

# To turn OFF:
sudo wg-quick down wg-admin-vm1
```

Step 2: Accessing Web Panels

1. In your browser, go to "Settings" -> "Privacy and security" -> "Certificates".
2. Select "Your certificates" and click "Import...".
3. Select the **admin_VM1.p12** file. The password is: **atakatak**.

Step 3: Install the Mumble Client

1. Update your package list in the terminal:

```
sudo apt update
```

2. Install the Mumble client:

```
sudo apt install mumble
```

3. Launch Mumble from your application menu or by typing `mumble` in the terminal.

Step 4: Mumble Client Configuration

1. In the Mumble client, go to "Configure" -> "Certificates" and import the **mumble-client_VM1.p12** file, using the **certificate password** provided below.
2. Add a new server, entering the IP address and port (default 64738).
3. Connect to the server. For the first connection, use the username **SuperUser** and the **server password** provided below.
4. Once logged in as SuperUser, you can register your normal username on the server.

Important Addresses & Passwords (VPN Access only)

Web UI Address: `https://10.166.0.7:8443`

Mumble Server Address: `10.166.0.7`

SERVER PASSWORD (for ATAK & Mumble SuperUser login): `nSkMeh5n3v84X6jn`

Mumble Certificate Password (.p12, for import): `TezSOBaQyYJNDOpe`

TAK Admin Login: `admin`

TAK Admin Password: `hZZxKwTXvNCMeh1!`

PostgreSQL Password: `WcGRERz1JMBMeh1!`