Network Lifecycle Audit Report

Pilot Assessment – NIS2 Compliance Review

Audit ID: AUD-20260625-000002 | **Date:** 2026-06-25 | **Snapshot:** 2026-06-25

NETWORK RISK STATUS

CRITICAL

Executive Summary

This network currently operates with **critical lifecycle and security exposure**.

- **3 / 10 devices (30.0%)** are operating beyond vendor support **(End of Life)**
- **9 / 10 devices (90.0%)** expose weak SNMP configuration
- **1 / 10 devices (10.0%)** lack centralized logging (Syslog)
- **1 / 10 devices (10.0%)** lack centralized authentication (AAA)

Unmanaged lifecycle and weak access control expose the network to **operational and security risks**.

[!] The current state is **not compliant with NIS2 requirements**. Immediate remediation is required within **30 days**.

Critical Findings (Top 10)

Device	IP Address	Lifecycle State	Risk Level	Explanation
s1-balmaz	10.237.3.253	End of Life	CRITICAL	No vendor patches or fixes available
s1-kecskemet	10.237.2.1	End of Life	CRITICAL	No vendor patches or fixes available
s1-szeged	10.237.15.2	End of Life	CRITICAL	No vendor patches or fixes available
s3-pm-a	10.237.65.5	Unknown	MEDIUM	Lifecycle data unavailable
s4-ecser-1	10.237.112.41	Unknown	MEDIUM	Lifecycle data unavailable

Configuration Gaps

Gap Type	Affected Devices	Network Coverage

AAA not configured	1 devices	10.0%
Syslog not configured	1 devices	10.0%
Weak SNMP configuration	**9 devices**	**90.0%**

Evidence Sample

```
[s1-balmaz] SNMP community string is weak or default
Source : config backup
Timestamp : 202602261359
snmp-server community public RO ACL-SNMP

[s1-szeged] SNMP community string is weak or default
Source : config backup
Timestamp : 202602261405
snmp-server community public RO ACL-SNMP

[s1-tiszaujvaros] SNMP community string is weak or default
Source : config backup
Timestamp : 202602261405
snmp-server community public RO ACL-SNMP
```