

EFESTO · NETWORK ANALYSIS AND PENETRATION TEST

# Seven-level network analysis and penetration test

A six-storey head office with dual Internet access, a single data centre and branch offices connected by VPN: from the project kick-off to the 30-day follow-up check.

## CLIENT

**Voltaria Distribuzione S.p.A. (example)**

## SECTOR

**Wholesale distribution of electrical materials and lighting**

## SCHEDULE

**Kick-off 28 April 2026 · tests 11 to 26 May 2026 (12 days)**

## VERSION

**1.0 · complete document**

## REFERENCES

**Mandate VD-2026-031 · follows from feasibility study SF-2026-014 (31 March 2026)**

## SERVICE

**Efesto — Advanced level**

## DELIVERY AND FOLLOW-UP

**Report 8 June 2026 · handover 10 June · follow-up check 8 July 2026**

## PREPARED BY

**BoNet™ — a Euro Buchberger project**

**Demonstration document.** Company name, people, connectivity suppliers, addresses, numbers and findings described in this report are invented for illustration and do not refer to any real client. BoNet™ publishes it as an example of the method, the level of detail and the organisation of a network analysis and penetration test engagement on a complex network. The report has a companion document, the feasibility study, which precedes it. The hardware and software listed represent the pool chosen for this simulated exercise: in a real engagement they are designed case by case.

# How to read this document

## CHAPTER 1 · COLOUR AND SYMBOL CONVENTION

Throughout the document colours have a fixed meaning. Anyone who learns them once can read any page without needing the legend: severity of findings, network zones, types of link and attention boxes use different colour families and are never confused. Every colour is always accompanied by a text or a code, so the document stays readable in black and white.

### 1.1 Severity of findings

Severity measures how much a finding can affect service continuity and data protection. It uses warm colours, from burgundy to green: **these colours appear only in findings** and never in network diagrams.

| Severity      | Meaning                                                                                           | Indicative time to act                                                           |
|---------------|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| CRITICAL      | Can cause a total outage, loss of data or full access by unauthorised people, with little effort. | Containment measures immediately (within 72 hours); permanent fix within 30 days |
| HIGH          | Serious impact on services or data, achievable with current skills.                               | Fix within 30 days                                                               |
| MEDIUM        | Limited impact, or achievable only under particular conditions.                                   | Fix within 90 days                                                               |
| LOW           | Minimal impact or conditions that are hard to achieve.                                            | At the next scheduled intervention                                               |
| INFORMATIONAL | An observation or good practice: no direct risk.                                                  | No action required                                                               |
| ✓ STRENGTH    | A successful design choice, to be maintained over time.                                           | —                                                                                |

The same warm colours also indicate the **operational risk** of a test day (chapter 6) and the level of project risks in the feasibility study. The **outcomes** of the delivery matrix (chapter 23) use blues and purples: **✓ MET** **⚠ WITH RESERVATION** **? TO BE VERIFIED**.

### 1.2 Network zones (diagrams)

In the diagrams each zone has its own colour, taken from the families of blues, purples, pinks and browns. The same colours return in the tables when talking about that zone.

| Zone                   | What it includes                                                                                             |
|------------------------|--------------------------------------------------------------------------------------------------------------|
| INTERNET AND SUPPLIERS | The lines of the two suppliers (Fibra Marmolada and Rete Lavaredo) and their modems, owned by the suppliers. |
| CLIENT EDGE            | The client's two routers, right after the modems, which speak BGP with the suppliers.                        |
| FIREWALL               | The high-availability firewall pair and the VPNs to the branches.                                            |
| DMZ                    | The intermediate zone with the services reachable from the Internet: mail, website, VPN concentrator.        |
| CORE · CED             | The two cores in failover, the servers, the backup: everything in the single data centre.                    |
| USERS (DATA)           | The network of employees' computers, on the six floors.                                                      |
| IP TELEPHONY           | One IP phone per user, on a dedicated voice network.                                                         |
| PRINTERS               | Ten printers per floor, on a dedicated network.                                                              |
| CAMERAS                | The cameras and the video recorder, on dedicated networks.                                                   |
| GUEST WI-FI            | Wi-Fi for guests, only in the ground-floor waiting room, isolated from the rest.                             |
| BONET TOOLS            | The test hardware, its connections and the points under test (T1-T6). <b>Gold is reserved for BoNet™.</b>    |

### 1.3 Links

Links are distinguished by the type of line, not by colour.

|                                                                                   |                                                                                        |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
|  | <b>Optical fibre</b> — vertical backbones, supplier lines, edge router links.          |
|  | <b>Copper Cat6</b> — horizontal cabling and links inside the CED.                      |
|  | <b>VPN</b> — encrypted tunnels between the branches and the firewall.                  |
|  | <b>Failover / high availability</b> — pairs of devices that take over from each other. |
|  | <b>BoNet test link</b> — temporary, only for the duration of the engagement.           |

1.4 Boxes and codes

**NOTE**

Clarifications and definitions of technical terms.

**ATTENTION**

A point that requires care, without being a prohibition.

**STOP · LIMIT NEVER TO BE CROSSED**

What is never done, or the condition in which work stops at once. Bright red is reserved for this use.

**RECOVERY**

What is done to return to normal, and who does it.

**TO BE DECIDED AT KICK-OFF**

A point that the client and BoNet™ settle together before starting.

**✓ STRENGTH**

A successful choice in the client's infrastructure.

**BONET TOOLS AND ACTIVITIES**

What BoNet™ installs and what it does.

**Codes.** **T1-T6:** points under test (floor switches chosen by the client) · **G1-G12:** test days · **R6-01:** finding of the level 6 analysis · **PT-03:** penetration test finding · **REI120:** compartment fire-resistant for 120 minutes · **HA:** high availability · **CED:** data centre (centro elaborazione dati).

# The scenario: Voltaria Distribuzione S.p.A.

## CHAPTER 2 · THE CLIENT AND ITS NETWORK

Voltaria Distribuzione S.p.A. (a fictitious name) is a wholesale distributor of electrical materials and lighting, with a six-storey head office and forty sales branches across Italy. The network was designed with care: redundancy from the lines to the floors, dual power supplies on every device, two physical routes for the fibre. It is a good starting point, and therefore a good test bed: a seven-level analysis and a penetration test show where redundancy really protects and where room for improvement remains.

### WHERE THIS ENGAGEMENT COMES FROM

On 9 March 2026 Voltaria put forward **eleven requests (R1–R11)**: fault tolerance, exposure from the Internet, risk from the floors and from guest Wi-Fi, inventory, branch VPNs, backups, an attestation for clients and the insurer, no halt to orders, a remediation plan, knowledge transfer, confidentiality. The **feasibility study SF-2026-014** (31 March 2026) assessed them and proposed option C, which this report documents. In chapter 23 each request receives its outcome.

## 2.1 The network in numbers

| Element            | Description in the example                                                                                                                                                                                                                                                    |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Internet access    | 4 fibre lines at 1 Gbit/s: 2 for each of the two suppliers ( <b>Fibra Marmolada</b> and <b>Rete Lavaredo</b> ), on two different terrestrial rings per supplier. 4 modems owned by the suppliers.                                                                             |
| Client edge        | 2 routers as a pair, outside the DMZ, right after the modems. They speak <b>BGP</b> with the suppliers: Voltaria has its own autonomous system (AS 64500) and its own block of public addresses (203.0.113.0/24). Numbers and addresses are those reserved for documentation. |
| Perimeter security | 2 firewalls in high availability (active/passive pair), a DMZ with mail, website and VPN concentrator, and 40 VPNs to the branches.                                                                                                                                           |
| Data centre (CED)  | A single room on the basement floor: 2 cores in failover, 3 virtualisation servers with 14 virtual machines (files, mail, business applications, directory), the backup system and the video recorder. All devices have dual power supplies.                                  |
| Building           | 6 floors (ground floor and floors 1–5), <b>2 switches per floor</b> : each connected to a different core and to each other, so that the loss of one core does not isolate the connected devices. 12 switches in total.                                                        |
| Users and devices  | 65 to 80 users per floor (433 in total), one IP phone per user (433), 10 printers per floor (60). 56 cameras on dedicated networks.                                                                                                                                           |
| Cabling            | Vertical fibre backbones in <b>two different risers, both REI120</b> ; horizontal copper Cat6 cabling.                                                                                                                                                                        |
| Wi-Fi              | Guests only, in the ground-floor waiting room, on an isolated network.                                                                                                                                                                                                        |

### ✓ STRENGTHS

Four lines on two suppliers and two rings; BGP at the edge; firewalls and cores in pairs; dual power supply everywhere; two REI120 risers for the fibre; separate networks for voice, printers, cameras and guests; Wi-Fi limited to what is strictly necessary.

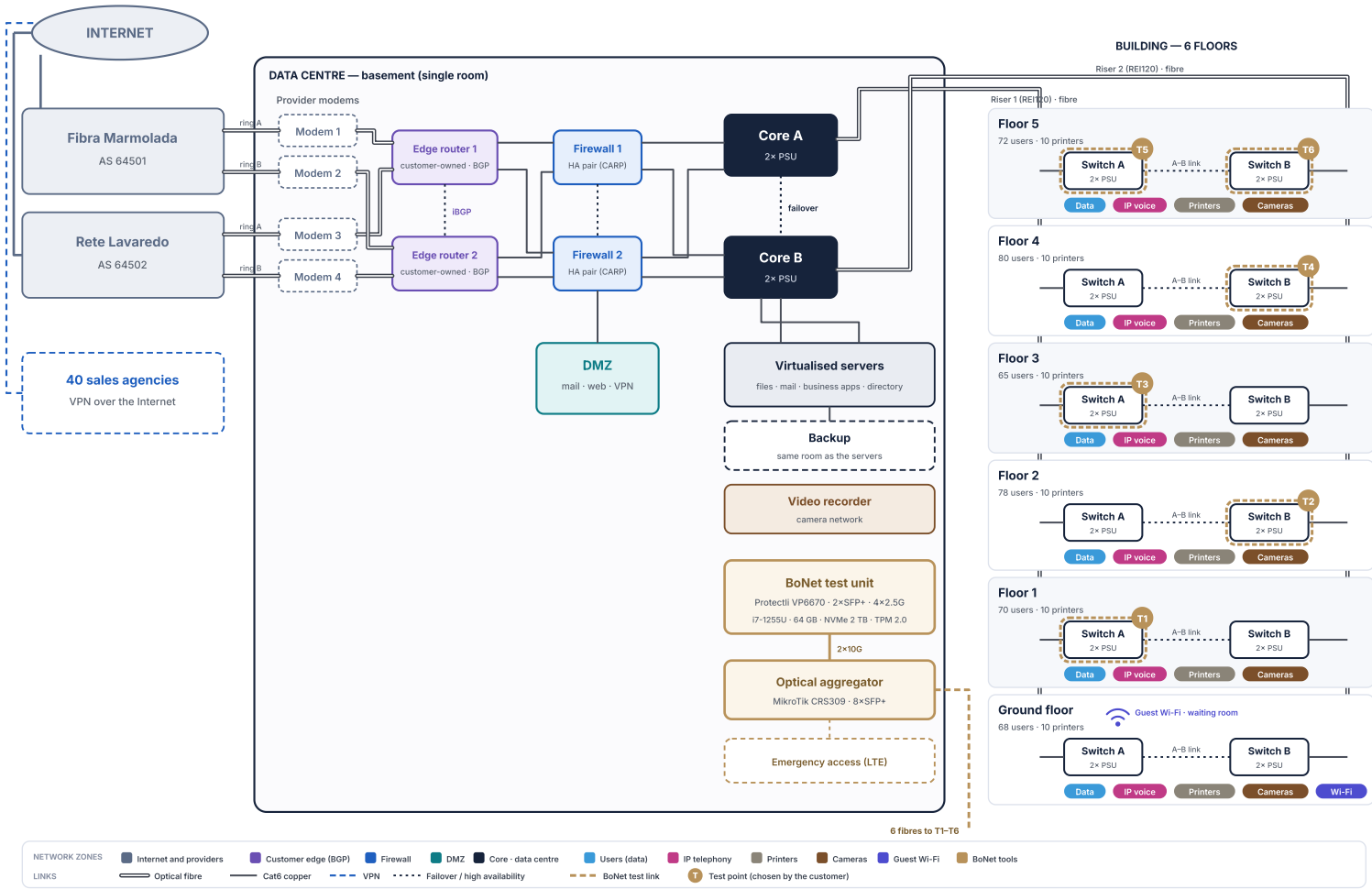
## 2.2 How the document is organised

The document is made up of three parts and four appendices. To read it in order, follow the chapters; to look up a topic, use the table.

| Ch.                                                                       | Contents                                                                                                                                                                           |
|---------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Part A — The project (starting from feasibility study SF-2026-014)</b> |                                                                                                                                                                                    |
| 1                                                                         | How to read this document: the colour convention                                                                                                                                   |
| 2–3                                                                       | The scenario and the general network diagram                                                                                                                                       |
| 4                                                                         | The project kick-off: roles, limits, stop conditions, recovery                                                                                                                     |
| 5                                                                         | Test hardware and software, with licences                                                                                                                                          |
| 6–7                                                                       | The test days; cabling to the floors (three options)                                                                                                                               |
| <b>Part B — The seven network analyses</b>                                |                                                                                                                                                                                    |
| 8–14                                                                      | Discovery and inventory · Topology and routing · Performance and capacity · Security and segmentation · Configuration and updates · Reliability and continuity · Intervention plan |
| <b>Part C — The penetration test (Efesto, Advanced level)</b>             |                                                                                                                                                                                    |
| 15–19                                                                     | External perimeter · Internal network and floors · Guest Wi-Fi, cameras, printers · Services and backup · Controlled exploitation and impact check                                 |
| 20–22                                                                     | Findings by severity · Clean-up and restoration · Remediation plan                                                                                                                 |
| 23                                                                        | <b>Handover: delivery and transfer</b> , with the traceability matrix of the study's requests                                                                                      |
| 24                                                                        | 30-day follow-up check                                                                                                                                                             |
| <b>Appendices</b>                                                         |                                                                                                                                                                                    |
| A–D                                                                       | Tool licences · Evidence log · Glossary · Legal aspects                                                                                                                            |

CHAPTER 3 · GENERAL NETWORK DIAGRAM

From the four lines to the twelve floor switches



The diagram shows Voltaria's network and, in gold, the BoNet™ tools installed for the engagement: the test unit in the CED, the optical aggregator with six fibres to the points under test T1-T6 (one on floors 1-4, two on floor 5) and the emergency access. Colours follow the convention of chapter 1.

# The project kick-off

## CHAPTER 4 · BEFORE EVERY CABLE AND EVERY TEST

A penetration test with hardware installed in the data centre is an **invasive** activity and, if not governed, **dangerous** for service continuity. The kick-off is the meeting — and the signed minutes that follow — in which it is decided **who does what, when and why**, which limits are never crossed and what is done if something goes wrong. Without a concluded and signed kick-off nothing is installed and no test is run.

The **starting point is feasibility study SF-2026-014**, delivered on 31 March 2026: it takes up its requests, assumptions, conditions and risks and turns them into signed decisions. It is the first item on the agenda.

### RULE OF ENGAGEMENT

No activity starts without the kick-off minutes signed by the client's sponsor and technical contact. Anyone involved, from Voltaria or BoNet™, can ask for a **stop** at any time, without having to explain why.

## 4.1 Who takes part and what they decide

| Role                         | In the example                 | Decides and does                                                                                                                                      | Presence                                              |
|------------------------------|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| Sponsor                      | Voltaria's general manager     | Signs the engagement and the authorisations; accepts the residual risk.                                                                               | Kick-off and closing                                  |
| Technical contact            | Head of information systems    | Approves plan, time windows and test points; can stop the tests; is the first contact for any anomaly.                                                | All days, on call                                     |
| Security and data protection | Privacy officer (DPO)          | Assesses the personal data involved; receives incident reports; handles the notifications required by law, which are the controller's responsibility. | Kick-off; on call                                     |
| Facilities manager           | Facility manager               | Power, cooling and access to the CED; passages through the REI120 risers.                                                                             | G1, G12 and on request                                |
| Qualified electrician        | Voltaria's trusted contractor  | Checks and provides the dedicated power supply; steps in for any electrical emergency.                                                                | G1 and G12 on site; other days on call within 2 hours |
| Certified cabler             | Voltaria's trusted contractor  | Cable runs, certification of the routes, restoration of the fire sealing of passages.                                                                 | G1 and G12 on site; other days on call within 2 hours |
| Connectivity suppliers       | Fibra Marmolada, Rete Lavaredo | Written consent to the checks on the external perimeter; technical reference for anomalies on the lines.                                              | Dedicated support number                              |
| BoNet™ project manager       | BoNet™                         | Runs the tests; <b>is on site during all risky activities and for any emergency or recovery</b> ; decides on stopping.                                | All days                                              |
| BoNet™ support technician    | BoNet™                         | Assists in the tests; keeps the evidence and the evidence log.                                                                                        | Test days                                             |

## 4.2 What is decided at the kick-off

| # | Decision                  | Why it matters                                                                                                                                   |
|---|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Feasibility study         | The requests R1-R11, the assumptions and the five conditions of study SF-2026-014 are confirmed or corrected; the outcome goes into the minutes. |
| 2 | Scope and objectives      | What is tested, from where and why; what stays out. What is not written is not touched.                                                          |
| 3 | Schedule and time windows | High-risk tests are done outside office hours or on quieter days; working days are reserved for non-invasive activities.                         |
| 4 | Operating limits          | The list of what is never done (box in this chapter).                                                                                            |
| 5 | Installation in the CED   | Rack space, power and cooling (dedicated box further on).                                                                                        |
| 6 | Cabling to the floors     | Which of the three options is used (chapter 7): existing spare routes, dedicated runs or mobile unit.                                            |

| #  | Decision                            | Why it matters                                                                                                                                                                                                                        |
|----|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7  | <b>The six switches under test</b>  | Chosen by the client: one on floors 1–4 and two on floor 5. For each, window, port and owner are set.                                                                                                                                 |
| 8  | <b>Third-party authorisations</b>   | Written consent of the connectivity suppliers and, if needed, of the building owner and the maintainer of the building systems. Voltaria confirms that it has informed its insurer (insurance is at its expense, as per the mandate). |
| 9  | <b>Safety prerequisites</b>         | Recent backup with a successful restore test; device configurations saved; list of critical services and their hours.                                                                                                                 |
| 10 | <b>Communications and on-call</b>   | Emergency directory, communication channel, response times, who informs whom.                                                                                                                                                         |
| 11 | <b>Licences and confidentiality</b> | List of tools with their licences (chapter 5, appendix A); non-disclosure agreement; handling and destruction of evidence.                                                                                                            |

#### TO BE DECIDED AT KICK-OFF · INSTALLATION IN THE CED: POWER AND HEAT

The test unit draws **12 W at idle and up to 100 W** under load (manufacturer's datasheet); the optical aggregator draws up to about 23–33 W (commercial sources differ: the final figure is the manufacturer's datasheet). The overall load, with a small dedicated UPS, is in the order of **200 W**, but it must still be agreed with the facilities manager: **(a)** a line or socket protected by a dedicated breaker, without connecting to PDUs already at their limit; **(b)** a dedicated UPS, sized for orderly shutdown; **(c)** position in the rack with free airflow and blanking panels to avoid recirculation; **(d)** reading of the intake air temperature before and after installation, with an agreed alert threshold (for example 27 °C at the rack intake) and shutdown of the BoNet™ unit if exceeded; **(e)** no disconnection of the client's devices to make room.

## 4.3 Operating limits and stop conditions

#### WHAT IS NEVER DONE

- No test that saturates the lines or the firewalls during working hours; no denial-of-service tests on production systems.
- No announcement or change of BGP routes: at the edge only configuration and exposure checks are done, read-only.
- No change to the client's production configurations: any change is the client's, at its decision.
- No opening or drilling of REI120 risers and compartments: only existing passages are used and only the cabler touches the openings.
- No access to personal data beyond the minimum needed to prove a finding; tests are recorded without copying the data.
- No test outside the approved scope and windows; no test on third-party systems without written consent.

#### STOP CONDITIONS · WORK STOPS AT ONCE IF

a service shows anomalies; the client receives an alarm; the temperature in the CED exceeds the threshold; a line, a core or a firewall is lost unexpectedly; the technical contact asks for it; a real security incident in progress is detected. **After a stop, work restarts only with the joint consent of the technical contact and the BoNet™ project manager.** Decisions are taken within 15 minutes.

## 4.4 Recovery plan

The plan says what is done if a test or an external event causes an interruption. It was agreed at the kick-off and is re-read at the start of every test day.

| Event                                              | Immediate action (within 5 minutes)                                            | Responsible                  | Restoration and check                                                                    |
|----------------------------------------------------|--------------------------------------------------------------------------------|------------------------------|------------------------------------------------------------------------------------------|
| <b>A core fails during a test</b>                  | Stop; no intervention by BoNet™; check that the surviving core holds the load. | Technical contact + BoNet™   | Restoration according to the client's procedure; return test only in a protected window. |
| <b>A line or a BGP session drops</b>               | Stop; BoNet™ does not act on the edge; the supplier is contacted if needed.    | Technical contact + supplier | Check of sessions and routes; resume only with consent.                                  |
| <b>Unexpected switchover between the firewalls</b> | Stop; check which firewall is active and the state of the VPN sessions.        | Technical contact            | Check of the branch VPNs and of the active rules.                                        |

| Event                                                        | Immediate action (within 5 minutes)                                                                       | Responsible            | Restoration and check                                                                                  |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------|
| <b>Temperature alarm or electrical overload in the CED</b>   | Shutdown of the BoNet™ unit by the button, with the emergency access (LTE) or from the dedicated breaker. | BoNet™ + electrician   | Measurement of temperature and power draw; restart only with the facilities manager's OK.              |
| <b>A floor switch does not respond</b>                       | BoNet™ disconnects the test link; the twin switch is checked.                                             | BoNet™ + IT            | Restoration from the saved configuration; check of the floor's phones, printers and workstations.      |
| <b>An application service slows down</b>                     | Stop and withdrawal of the test traffic.                                                                  | BoNet™ + IT            | Root-cause analysis; resume with a new OK.                                                             |
| <b>Damage to a cable or to an REI120 passage</b>             | Work stops in the area.                                                                                   | Cabler + facilities    | Documented restoration and testing, including fire sealing, before reopening the area.                 |
| <b>A security incident already in progress is discovered</b> | Stop; immediate notice to the sponsor and the DPO; tests are not touched.                                 | Sponsor + DPO + BoNet™ | The controller handles the notifications required by law; BoNet™ supports with the evidence collected. |
| <b>Loss or theft of the test unit</b>                        | The client is informed immediately; the disk is encrypted and protected by the TPM.                       | BoNet™                 | Revocation of credentials and accesses used in the tests; written report within 24 hours.              |

#### RECOVERY · ON-SITE PRESENCE

The BoNet™ project manager is **on site** during all risky activities and for any emergency or recovery. The electrician and the cabler are on site on days G1 and G12 and reachable within 2 hours on other days. The client guarantees access to the CED for the whole duration of the engagement.

#### 4.5 WHAT THE KICK-OFF PRODUCES

The **signed minutes**, which confirm or update the feasibility study, with scope, schedule, limits and choice of cabling · the **test and recovery plan**, with the emergency directory · the **list of licences** of the tools (appendix A) · the **third-party authorisations** (connectivity suppliers, building owner, maintainers) · the **initial survey** of the CED: temperature, power draw and state of the backups.

# Test hardware and software

## CHAPTER 5 · WHAT BONET™ INSTALLS AND THE TOOLS IT WORKS WITH

For this engagement BoNet™ installs a dedicated test unit in Voltaria's CED, with fibre links to six floor switches chosen by the client. The pool described here is the one chosen for this **simulated exercise**: in a real engagement it is designed case by case, according to what is being done and for which infrastructure, and can be heavier or lighter.

### BONET™ TOOLS AND ACTIVITIES · THE POOL IS PROPORTIONATE TO THE ENGAGEMENT

A home network, a professional practice or a six-storey company require different equipment. That is why, before every real engagement, BoNet™ defines the pool, buys or rents the necessary tools, puts the licences in BoNet™'s name and lists them at the kick-off and in the final report. The tools in this chapter are the ones we would use here.

## 5.1 Hardware

| ID  | Component                               | Model                                                                                             | Function and main features                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----|-----------------------------------------|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| H1  | <b>Main test unit</b> , in the CED      | <b>Protectli Vault Pro VP6670</b><br>✓ data from the manufacturer's datasheet (15/12/2025)        | Runs scans and collects the evidence. Intel Core i7-1255U (10 cores, 12 threads); <b>2 SFP+ 10G ports</b> (Intel X710-BM2) and 4 × 2.5G ports (Intel i226-V); DDR5 memory up to 64 GB ( <b>64 GB configured</b> ); NVMe M.2 2280 disk ( <b>2 TB configured, encrypted</b> ); optional <b>TPM 2.0 module</b> (installed); M.2 slot for an <b>LTE</b> module with SIM (installed: emergency access). Consumption 12 W at idle and 100 W at most; operating temperature from -10 to +50 °C; 191 × 178 × 76 mm. It has two internal fans: it is not a fanless device. |
| H2  | <b>Optical aggregator</b> , in the CED  | <b>MikroTik CRS309-1G-8S+IN</b><br>✓ data from retailers' datasheets; consumption to be confirmed | 8 SFP+ 10G ports and one 1G management port, passive cooling. <b>2 ports</b> to H1 (20 Gbit/s aggregated) and <b>6 ports</b> to the points under test T1-T6: these are the six fibres of the engagement. Maximum consumption 23-33 W (sources differ: the manufacturer's datasheet prevails).                                                                                                                                                                                                                                                                     |
| H3  | <b>Spare unit</b>                       | A second VP6670, configured like H1                                                               | Replaces H1 in case of failure, without losing test days.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| H4  | <b>External observation point</b>       | Server in a data centre in Italy, with a fixed address (to be chosen at kick-off)                 | For the “from the Internet” tests: Voltaria's perimeter is observed from outside, not from its network.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| H5  | <b>SFP+ optical modules</b>             | 10G SR (multimode OM4) and 10G LR (single-mode OS2) (to be defined)                               | Eight modules plus spares, chosen after surveying the client's fibre and switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| H6  | <b>Cables and test gear</b>             | OM4 and OS2 fibre patch cords, Cat6 reels, tools to certify copper and fibre                      | For the dedicated runs (chapter 7) and for continuity checks: handled by the cabler.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| H7  | <b>Passive network TAPs</b>             | Copper and fibre (to be defined)                                                                  | They allow traffic to be observed without interrupting it.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| H8  | <b>Dedicated UPS and power metering</b> | Compact UPS with metered PDU (to be defined)                                                      | Orderly shutdown and measurement of the power draw throughout the engagement.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| H9  | <b>Mobile unit</b>                      | Laptop with SFP+ and Ethernet adapters (to be defined)                                            | For cabling option C: it connects directly to the floor switch, with no cable runs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| H10 | <b>Wi-Fi adapter</b>                    | USB, with monitor mode (to be defined)                                                            | For the checks on guest Wi-Fi (day G9).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

### NOTE · IS ONE UNIT ENOUGH?

For the tests from the CED a single unit is enough: 10 cores, 64 GB of memory and 20 Gbit/s to the aggregator comfortably handle the loads of this engagement, which are limited by choice. But an invasive engagement does not rely on a single device: that is why the pool includes the spare unit (H3), the external observation point (H4), the emergency access (LTE) and the Wi-Fi adapter (H10).

## 5.2 Software

| Function                               | Tool                                                                                         | Licence                                                   | Notes                                                                                 |
|----------------------------------------|----------------------------------------------------------------------------------------------|-----------------------------------------------------------|---------------------------------------------------------------------------------------|
| <b>Base system</b>                     | Kali Linux (rolling release, official image)                                                 | Free software (various licences, mostly GPL)              | Encrypted disk; image verified with the producer's signature before use.              |
| <b>Inventory and scanning</b>          | Nmap                                                                                         | Nmap Public Source License                                | Detection of devices, ports and services, at an agreed limited speed.                 |
| <b>Vulnerability assessment</b>        | Greenbone Community Edition (OpenVAS) · <b>Tenable Nessus Professional</b>                   | GPL · <b>commercial</b> , annual subscription per scanner | Two different engines, to compare results and eliminate false alarms.                 |
| <b>Traffic analysis</b>                | Wireshark · Zeek · Suricata                                                                  | GPLv2 · BSD · GPLv2                                       | Also to understand whether the client's systems notice the tests.                     |
| <b>Web applications and encryption</b> | <b>Burp Suite Professional</b> (PortSwigger) · testssl.sh                                    | <b>Commercial</b> , annual subscription per user · GPLv2  | Checks of website, mail and portals; strength of the encryption.                      |
| <b>Directory and identity</b>          | <b>PingCastle</b> (Netwrix) · BloodHound Community Edition (SpecterOps)                      | <b>Commercial</b> for consultants · Apache 2.0            | Health of the corporate directory and privilege paths.                                |
| <b>Wi-Fi</b>                           | Kismet                                                                                       | GPLv2                                                     | Detection and verification of the guest network.                                      |
| <b>Performance</b>                     | iperf3                                                                                       | BSD                                                       | Speed measurements between the floors and the CED, in agreed windows.                 |
| <b>Evidence log</b>                    | Synchronised clock (NTP), session recording, SHA-256 fingerprint of files, encrypted archive | BoNet™ internal procedures                                | Every test has date, time, operator and fingerprint: it can be repeated and verified. |

The tools for controlled exploitation (day G11) are not listed here: they are chosen case by case and agreed at the kick-off, one test at a time, with the technical contact's consent.

### LICENCES · HOW WE MANAGE THEM

Every commercial licence is **purchased for the engagement** and registered in BoNet™'s name (not the client's). Licence type, number and expiry are presented **at the kick-off** and reported in the **final report** (appendix A). Tool versions are those in force at the start of the engagement and are frozen until closure, so that results are repeatable.

# The test days

CHAPTER 6 · TWELVE FULL DAYS, ONE AFTER THE OTHER

The test is spread over **twelve full days**, from 11 to 26 May 2026, preceded by the kick-off (28 April) and followed by the report (8 June), the handover (10 June) and a follow-up check after thirty days (8 July). The most delicate days take place with the BoNet™ project manager on site and, where needed, with the electrician and the cabler. Every day starts with a re-reading of the recovery plan and ends with a check that everything is back as before.

| Day | Activity                                                                                                                                                                                     | Where                  | Operational risk | Others present besides BoNet™                |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|------------------|----------------------------------------------|
| G1  | <b>Installation in the CED.</b> Placing H1 and H2, electrical and thermal checks, connecting the fibres, continuity tests. No testing.                                                       | CED                    | MEDIUM           | Electrician, cabler, facilities, IT          |
| G2  | <b>Inventory and topology</b> (levels 1 and 2): passive discovery, diagram check, basic performance measurements.                                                                            | CED                    | LOW              | IT                                           |
| G3  | <b>External perimeter, part 1.</b> Observation from outside (H4): published services, DMZ, mail and website.                                                                                 | External               | LOW              | IT                                           |
| G4  | <b>External perimeter, part 2.</b> Edge routers and BGP sessions (read-only configuration checks only), firewall, branch VPNs.                                                               | External + CED         | MEDIUM           | IT; suppliers on call                        |
| G5  | <b>Internal network from the CED.</b> Separation between data, voice, printers, cameras and management; firewall rules.                                                                      | CED                    | MEDIUM           | IT                                           |
| G6  | <b>Floors 1 and 2</b> (points T1 and T2): tests from the access ports, network isolation, printers. Outside office hours.                                                                    | Floors 1–2             | MEDIUM           | IT, cabler on call                           |
| G7  | <b>Floors 3 and 4</b> (points T3 and T4): tests from the access ports, IP phones, workstations. Outside office hours.                                                                        | Floors 3–4             | MEDIUM           | IT, cabler on call                           |
| G8  | <b>Floor 5</b> (points T5 and T6, the two switches): tests from the access ports and <b>failover test</b> between switches A and B, only in a protected, agreed window.                      | Floor 5                | HIGH             | IT, electrician and cabler on call           |
| G9  | <b>Guest Wi-Fi, cameras and printers.</b> Isolation of the guest network, dedicated networks, management interfaces.                                                                         | Ground floor + CED     | LOW              | IT                                           |
| G10 | <b>Services and backup.</b> Mail, files, directory, business applications; access to the backup system and state of the copies.                                                              | CED                    | MEDIUM           | IT                                           |
| G11 | <b>Controlled exploitation and impact check.</b> One test at a time, only for points already identified, with the technical contact's consent.                                               | Depending on the point | HIGH             | IT, DPO, electrician on call                 |
| G12 | <b>Clean-up and restoration.</b> Removal of every file, account or configuration created by the tests; check of the return to the initial state; uninstalling the hardware; closing meeting. | CED + floors           | MEDIUM           | Electrician, cabler, facilities, IT, sponsor |

NOTE · OPERATIONAL RISK

The “Operational risk” column uses the same colours as the severity of findings, but it means something else: **how much a day can affect the service if something goes wrong**. The highest-risk days (G8 and G11) take place in protected windows, with the recovery plan already open on the table.

## After the tests

| When           | What                                                                                                                                                                            |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| By 8 June 2026 | Report with findings by severity, evidence, impact and recommended fixes; presentation to the sponsor and the technical contact.                                                |
| 10 June 2026   | <b>Handover:</b> delivery and transfer to Voltaria's IT team, with the traceability matrix of the feasibility study's requests (chapter 23).                                    |
| 8 July 2026    | Follow-up check (Advanced level): the tests are repeated on the corrected points, with a short update of the report. A new installation of the hardware is agreed case by case. |

# Cabling to the floors: three options

CHAPTER 7 · HOW THE SIX SWITCHES UNDER TEST ARE REACHED

The test unit in the CED must be able to reach the six switches chosen by the client (T1–T6, on floors 1–5): six routes from the CED to the floors are therefore needed. There are three ways to have them. **The main approach uses the spare routes that the client has already set up in case of failure**; if they cannot be used, we move to dedicated runs, and lastly to the mobile unit. The choice is made at the kick-off, after a survey of the existing cabling.

**A · Existing spare routes**  
*main approach*

**What.** Fibre pairs or cables that Voltaria has already laid as spares for failures, in the two REI120 risers or in the vertical cabling.

**When.** If at the kick-off they turn out to be free, labelled, certified and usable without reducing the spare capacity below the agreed limit.

**Who.** The client's cabler checks and certifies the routes; BoNet™ connects them to the six ports of the aggregator.

**Advantages.** Lower cost, no new cables, no new work in the risers, short times.

**Caution.** The spare is the client's parachute: while it is in use, the reserve is reduced. Return within 4 hours on request is agreed, and continuity is checked before and after.

LOWER COST

**B · Dedicated runs**

**What.** New routes laid only for the engagement, from the CED to the six switches, using existing passages.

**When.** If the spare routes do not exist, are not free, or the client prefers not to commit them.

**Who.** Certified cabler, with electrician and facilities where needed. Restoring the fire sealing of the openings is the cabler's job, documented.

**Advantages.** Independence from the spare; routes and lengths chosen for the test.

**Caution.** Higher cost (materials, labour, testing); longer times; authorisation to use the REI120 passages is needed; removal or retention of the routes to be agreed at the end of the engagement.

HIGHER COST

**C · Mobile unit**

**What.** A laptop with adapters (SFP+ and Ethernet) that connects directly to the floor switch port, without cable runs.

**When.** If A and B are not practicable, or for spot checks at more points than the six.

**Who.** BoNet™, with the IT contact; the cabler remains on call.

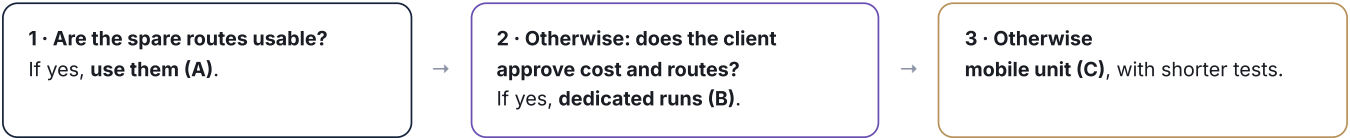
**Advantages.** No works; flexible; installed in a few minutes.

**Caution.** The mobile unit is not connected to the CED: tests are shorter and less complete (no continuous capture, no immediate correlation with the main unit) and require physical presence at each floor, outside office hours.

LOWER COST

MORE BONET™ PRESENCE

## How to choose



# Level I · Discovery and inventory

CHAPTER 8 · PART B — THE SEVEN NETWORK ANALYSES

The first level answers a simple question: **what is really on the network?** Before judging anything, the inventory Voltaria had is compared with what the devices themselves say is connected. The differences are not errors to blame on anyone: they are the starting point for having, for the first time, a list that can be trusted (request R4). The activity took place on day G2, during working hours, passively, without sending any traffic beyond the normal.

O  
CRITICAL

I  
HIGH

I  
MEDIUM

I  
LOW

I  
STRENGTH

## 8.1 What was compared

On one side, Voltaria's list (a spreadsheet last updated in January 2025, plus the network diagram). On the other, what emerges from the devices' tables (MAC and ARP addresses of the switches and cores, DHCP leases, the hypervisor's list of virtual machines) and from a week of passive scanning. Every device was matched to a category, a floor and a network.

| Category                                        | On the list | Detected | Difference |
|-------------------------------------------------|-------------|----------|------------|
| Workstations (computers)                        | 433         | 441      | +8         |
| IP phones                                       | 433         | 433      | 0          |
| Printers and multifunction devices              | 60          | 62       | +2         |
| Cameras and video recorder                      | 57          | 57       | 0          |
| Floor switches and cores                        | 14          | 14       | 0          |
| Firewalls and edge routers                      | 4           | 4        | 0          |
| Physical servers and virtual machines           | 17          | 19       | +2         |
| Wi-Fi access points (guests)                    | 2           | 2        | 0          |
| Managed backup system and UPS                   | 4           | 4        | 0          |
| Other devices (displays, badge readers, clocks) | 21          | 29       | +8         |
| Total                                           | 1,045       | 1,065    | +20        |

✓ STRENGTH

All the devices that hold the network up (switches, cores, firewalls, edge routers, physical servers) are on the list, with name, role and floor. The inventory is reliable where it matters most.

## 8.2 Findings

| ID    | Severity | Title                                                                | What we observed                                                                                                                                                                       | What we recommend                                                                                                                                        |
|-------|----------|----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| R1-01 | HIGH     | Virtual machine with an operating system that is no longer supported | Of the two virtual machines not on the list, one uses an operating system that the vendor no longer updates. It belongs to an old project and is reachable from the server network.    | Identify the owner; if it is not needed, shut it down and archive it; if it is needed, update it or isolate it in a separate network with minimal rules. |
| R1-02 | MEDIUM   | Twenty devices not in the inventory                                  | Eight computers, two printers, two virtual machines and eight miscellaneous devices (displays, badge readers) are connected but are not on the list. For some, the owner is not known. | Match each device to a person; add it to the inventory; for those without an owner, disconnect them after notice.                                        |
| R1-03 | LOW      | Wall-socket labels not aligned                                       | In three floor cabinets, about one socket in ten has a label different from the name in the switch table.                                                                              | Relabel in half a day's work, with the cabler; keep the table as the single source.                                                                      |

The eight extra computers include laptops of guests and of external technicians connected on the floors. Device identifiers (MAC addresses) stay in the evidence log, not in this document.

**NOTE · HOW TO READ THE "+20"**

Twenty devices out of 1,045 is less than 2%: for a site of four hundred people it is an average result. The point is not the number, but knowing **who is responsible** for each one and why it is connected.

# Level 2 · Topology and routing

CHAPTER 9 · PART B — THE SEVEN NETWORK ANALYSES

The second level checks **how traffic finds its way**: physical and logical links, routing towards the Internet, behaviour of the device pairs. The official diagram is compared with the one rebuilt from the devices. At the edge, towards the suppliers, only **read-only** checks were done: no route was announced, changed or withdrawn. Activity of day G2, with the technical contact present and the supplier on call.

O  
CRITICAL

O  
HIGH

I  
MEDIUM

2  
LOW

2  
INFORMATIONAL AND  
STRENGTHS

## 9.1 The network as we see it

| Segment             | What we checked                                                                                                                                                            | Outcome       |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Lines and suppliers | Four stable BGP sessions, two per supplier. Voltaria's block of public addresses (203.0.113.0/24) and autonomous system number (AS 64500) are announced by both suppliers. | ✓ AS DESIGNED |
| Edge filters        | The routers accept from the suppliers only the expected prefixes and have a limit on the number of routes received per session.                                            | ✓ STRENGTH    |
| Firewall pair       | The switchover between active and passive is documented; the state of the VPN sessions is synchronised between the two.                                                    | ✓ AS DESIGNED |
| Cores and floors    | Every floor has two switches on different cores, linked to each other. Each floor's path to the data centre is doubled.                                                    | ✓ AS DESIGNED |
| Official diagram    | Four differences from Voltaria's diagram (a link between switches not shown, two port labels, a network no longer in use), corrected in the diagram delivered.             | INFORMATIONAL |

✓ STRENGTH

Prefix filters and route limits at the edge (BGP): an error by a supplier, or an unwanted announcement attempt, does not enter Voltaria's network.

## 9.2 Findings

| ID    | Severity | Title                                          | What we observed                                                                                                                                                                                                           | What we recommend                                                                                                                               |
|-------|----------|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| R2-01 | MEDIUM   | Spanning tree root not fixed                   | The switch that coordinates each floor's network (the "root") is chosen by the devices themselves and not by a client rule: a new device, or one restored with factory settings, could become the root and divert traffic. | Fix the root with an explicit priority on the cores, and the backup root on the second core; enable protection on the access ports.             |
| R2-02 | LOW      | Unbalanced exit to the Internet                | The exit preferences send almost all traffic over one supplier's lines (Fibra Marmolada); the other supplier (Rete Lavaredo) is used mainly in case of failure.                                                            | Consider splitting traffic by service (for example, VPN and mail on one supplier, the rest on the other) after measuring the load (chapter 10). |
| R2-03 | LOW      | Three static routes to decommissioned networks | Three routes remain on the firewall towards networks that no longer exist: they do no harm today, but they confuse whoever reads the configuration.                                                                        | Remove them at the next scheduled intervention, after checking that they are useless.                                                           |

The checks on the BGP sessions were carried out with the written consent of both suppliers and remained read-only. The consent is part of the kick-off documentation.

# Level 3 · Performance and capacity

CHAPTER 10 · PART B — THE SEVEN NETWORK ANALYSES

The third level measures **how loaded the links and devices are** and how much margin remains, ahead of new services such as the order portal Voltaria will open in July. The data come from two sources: the devices' counters over two weeks, and active speed and delay measurements in agreed windows, at limited intensity. No test saturated a line or a device during working hours.



10.1 Load and margin

| Link or device                   | Capacity | Average load · peak  | Comment                                                                                                  |
|----------------------------------|----------|----------------------|----------------------------------------------------------------------------------------------------------|
| Internet lines (4 × 1 Gbit/s)    | 4 Gbit/s | 14% · 61% (outbound) | The peak is on a single line, in the early afternoon, when orders and copies go out.                     |
| Core–floor backbones (10 Gbit/s) | 12 × 10  | 3% · 11%             | Very wide margin.                                                                                        |
| Link between the two cores       | 2 × 10   | 2% · 7%              | Very wide margin.                                                                                        |
| Firewall (processor)             | —        | 24% · <b>71%</b>     | With intrusion detection active and 40 VPNs, the peak rises close to the recommended threshold (70–75%). |
| Floor–CED delay                  | —        | < 1 ms               | No difference between floors.                                                                            |
| Guest Wi-Fi (2 points)           | —        | up to 14 devices     | Capacity adequate for the waiting room.                                                                  |

✓ STRENGTH

The backbones between cores and floors and the link between the cores work at a small fraction of their capacity: the internal network can grow a lot without intervention.

10.2 Findings

| ID    | Severity | Title                                          | What we observed                                                                                                         | What we recommend                                                                                                                                                                                |
|-------|----------|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| R3-01 | MEDIUM   | Reduced margin on the firewall                 | The firewall's processor reaches 71% at peaks. The July order portal and the new VPNs will increase the load.            | Before July: measure the load with the portal in trial; consider replacing it with a more powerful model or moving intrusion detection elsewhere; calculate the margin with at least 30% growth. |
| R3-02 | LOW      | Quality of service for phone calls not uniform | On floors 2 and 5 calls do not have priority over data traffic: it is not noticeable now, but it would be during a peak. | Apply the same priority rule on all floor switches.                                                                                                                                              |

# Level 4 · Security and segmentation

CHAPTER 11 · PART B — THE SEVEN NETWORK ANALYSES

The fourth level looks at **how the network is divided into zones and who can talk to whom**. Good segmentation limits damage: if a device is compromised, it does not reach everything. Here the firewall rules, the virtual networks (VLANs) and the management interfaces are examined by **reading the configurations**, without testing anything. The real tests, from the inside, are in part C of this document. Activity of days G2 and G5.

O  
CRITICAL

I  
HIGH

2  
MEDIUM

I  
LOW

2  
STRENGTHS

## 11.1 The zones and who can talk to whom

The table shows the flows allowed between zones, as they result from the rules in force. **Yes**: allowed by design. **No**: blocked. **Exception**: allowed beyond the design intent (see the findings).

| From → to | USERS         | VOICE | PRINTERS | CAMERAS        | GUESTS | SERVERS             | MANAGEMENT | DMZ | INTERNET    |
|-----------|---------------|-------|----------|----------------|--------|---------------------|------------|-----|-------------|
| USERS     | —             | No    | Yes      | No             | No     | Yes                 | Exception  | Yes | Yes         |
| VOICE     | No            | —     | No       | No             | No     | Yes (telephony)     | No         | No  | Yes (lines) |
| PRINTERS  | Yes (replies) | No    | —        | No             | No     | Yes (queues)        | No         | No  | No          |
| CAMERAS   | No            | No    | No       | —              | No     | Yes (recorder)      | Exception  | No  | No          |
| GUESTS    | No            | No    | No       | No             | —      | No                  | No         | No  | Yes         |
| SERVERS   | Yes (replies) | Yes   | No       | Yes (recorder) | No     | —                   | Yes        | Yes | Yes         |
| DMZ       | No            | No    | No       | No             | No     | Yes (services only) | No         | —   | Yes         |

✓ STRENGTHS

- **Well-thought-out zones.** Voice, printers, cameras and guests are on separate networks, with “deny all” starting rules and explicit openings.
- **Isolated DMZ.** The zone of public services can reach the servers only on the necessary services and does not reach the users' networks.

## 11.2 Findings

| ID    | Severity | Title                                                   | What we observed                                                                                                                                                                                                         | What we recommend                                                                                                                              |
|-------|----------|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| R4-01 | HIGH     | Management network reachable from users                 | A rule allows the users' network to reach the administration interfaces of servers and devices (backup system included). It was a temporary opening that remained in force. It is the underlying cause of finding PT-01. | <b>Immediately:</b> restrict access to two administration workstations. <b>Then:</b> a separate management network, reachable only from there. |
| R4-02 | MEDIUM   | Video recorder management port towards the data network | The video recorder has two ports: one on the camera network, one on the data network for management. Thus the camera network has a path to the data network. Verified in practice with finding PT-07.                    | Move the recorder's management to the management network; explicit rule between the two networks; leave no other ports.                        |
| R4-03 | MEDIUM   | No authentication of devices on access ports            | Whoever connects a device to a socket gets a network according to the port, without the device identifying itself. If a device is replaced or a switch is left behind, no check reports it.                              | Introduce device authentication on ports (802.1X) in phases: first the floors with the most guests, then the others.                           |

| ID    | Severity | Title                 | What we observed                                                                                     | What we recommend                                                                     |
|-------|----------|-----------------------|------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| R4-04 | LOW      | Unused firewall rules | Twenty-three rules out of 187 have had no traffic for over six months, and many have no description. | Clean-up: disable, observe for a month, remove; mandatory description for every rule. |

# Level 5 · Configuration and updates

CHAPTER 12 · PART B — THE SEVEN NETWORK ANALYSES

The fifth level checks **how the devices are configured and how up to date they are**. A configuration that is correct today can become a problem tomorrow if a security update does not reach a device: for this reason settings, software versions and the way updates are distributed are examined together. Activity of days G2 and G5, on the saved configurations and on the versions the devices declare, without changing them.

O  
CRITICAL

I  
HIGH

2  
MEDIUM

2  
LOW

I  
STRENGTH

## 12.1 Software versions of the devices

Versions were read from the devices and compared with the reference version Voltaria has set itself (the latest one with the known security fixes). The numbers are in generic form; the detail is in the evidence log.

| Family                        | Devices    | Aligned  | Notes                                                               |
|-------------------------------|------------|----------|---------------------------------------------------------------------|
| Cores                         | 2          | 2 of 2   | Updated in a maintenance window in January.                         |
| Floor switches                | 12         | 11 of 12 | The floor 4 switch is one security version behind (finding R5-01).  |
| Firewalls and edge routers    | 4          | 4 of 4   | —                                                                   |
| Mail server in the DMZ        | 1          | 0 of 1   | Updates four months behind (finding R5-02).                         |
| Other servers and hypervisors | 3 + 19 VMs | 20 of 22 | Two virtual machines not updated; one is the one in finding R1-01.  |
| Printers                      | 62         | 41 of 62 | Old firmware: a topic also covered in the penetration test (PT-02). |

## 12.2 Findings

| ID    | Severity | Title                                                   | What we observed                                                                                                                                                                                                                                                                              | What we recommend                                                                                                                                                   |
|-------|----------|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| R5-01 | HIGH     | Switch updates with no completeness check               | Floor switches are updated by a scheduled procedure. The floor 4 switch was powered off for maintenance at the time of the last update and did not receive it; the procedure neither reported the device as not reached nor retried. The finding is proven in practice by PT-03 (chapter 16). | The procedure must report the devices not reached, retry, and produce a report for IT; automatic comparison with the reference version; monthly check with minutes. |
| R5-02 | MEDIUM   | Updates behind on the mail server                       | The mail server in the DMZ has four months of security updates not applied; it has no scheduled maintenance window.                                                                                                                                                                           | Monthly window agreed with the company; apply the critical ones at once; test on a copy before production.                                                          |
| R5-03 | MEDIUM   | Shared administration account                           | On the network devices a single administration account is used, known to five people: it is not possible to tell who did what.                                                                                                                                                                | Personal accounts, with centralised authentication; an emergency account kept safe and used only when needed.                                                       |
| R5-04 | LOW      | SNMP management with default parameters on some devices | Six devices (printers and an uninterruptible power supply) respond with the factory access string to the monitoring protocol.                                                                                                                                                                 | Move to the version with authentication and encryption; disable where not needed.                                                                                   |
| R5-05 | LOW      | Device logs not centralised                             | Logs are kept on each device for about 30 days, and not in a common archive.                                                                                                                                                                                                                  | Centralised archive with retention of at least 12 months and alerts on important events.                                                                            |

✓ STRENGTH

The configurations of all network devices are saved every night with change history: in case of failure or error, rollback takes minutes. This good practice made possible the fast restoration provided for by the recovery plan (chapter 4).

# Level 6 · Reliability and continuity

CHAPTER 13 · PART B — THE SEVEN NETWORK ANALYSES

The sixth level measures how much the network keeps working when something breaks, and how long it takes to return to normal. It looks at the redundancy of devices, lines, power, physical routes and data. For Voltaria the picture is good: single failures are almost all covered. The margins for improvement concern mainly the events that hit **the whole data centre at once**.



✓ STRENGTHS

- **Internet access.** Four lines on two suppliers and two rings each, with BGP: the loss of a line, a ring or an entire supplier does not change Voltaria's public addresses.
- **Devices.** Edge routers, firewalls and cores in pairs; dual power supply everywhere.
- **Floors.** Two switches per floor, on different cores and linked to each other: the loss of a core does not isolate the floor.
- **Physical routes.** Two distinct REI20 risers for the fibre: a physical fault in one does not interrupt the other.

## 13.1 Findings

| ID    | Severity      | Title                                  | What we observed                                                                                                                                                                                                               | What we recommend                                                                                                                                             |
|-------|---------------|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| R6-01 | HIGH          | Data centre in a single room           | Cores, firewalls, servers and backup are in the same room: a local event (fire, flooding, failure of the air-conditioning or the electrical system) would stop everything, despite the duplicated devices.                     | Continuity plan; a secondary room for essential services and for the copies; in the short term, smoke and flood detection and an off-site copy of the data.   |
| R6-02 | HIGH          | Backup in the same room as the servers | The copies are only in the CED, with no off-site copy and no immutable copy. The last full restore test dates back 14 months.                                                                                                  | The 3-2-1 rule (three copies, two media, one off-site); encrypted off-site copy; immutable copy; restore test every quarter.                                  |
| R6-03 | MEDIUM        | Dual power on the same line            | The two power supplies of the cores are connected to PDUs powered by the same UPS: they protect against a power-supply failure, not against that of the UPS or the electrical line.                                            | Two independent electrical lines (A and B) with separate UPSs; periodic test of unplugging one line.                                                          |
| R6-04 | MEDIUM        | Devices with a single connection       | IP phones, printers and computers have a single cable: if a floor switch fails, the devices connected to it lose the network. The twin switch protects against the failure of the core, not of the individual device's switch. | Distribute the critical points (reception, meeting rooms, printers, management phones) between switch A and switch B; keep a spare switch already configured. |
| R6-05 | LOW           | Failover tests not repeated            | The last documented switchover test between cores, firewalls and edge routers dates back more than 12 months.                                                                                                                  | A calendar of tests at least yearly, in a protected window, with minutes.                                                                                     |
| R6-06 | INFORMATIONAL | Spare routes labelled                  | The spare routes in the risers exist and are labelled: useful for failures and for the test cabling.                                                                                                                           | Keep the documentation up to date.                                                                                                                            |

### 13.2 One finding in detail

|                     |                                                                                                                                                                                                                                                                                                |                              |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| R6-01               | HIGH                                                                                                                                                                                                                                                                                           | Data centre in a single room |
| WHAT                | All the devices that run the network and the data (cores, firewalls, servers, backup, test access) are in the same room, on the basement floor.                                                                                                                                                |                              |
| WHY IT MATTERS      | The redundancy of devices protects against the failure of a component. It does not protect against an event that hits <b>the whole room</b> : in that case the two cores, the two firewalls and the backup copies are out of service together.                                                 |                              |
| HOW WE VERIFIED IT  | Site visit to the CED (G1), review of the electrical diagram, of the fire-protection documentation and of the position of the backup systems.                                                                                                                                                  |                              |
| IMPACT              | Total outage of the head office and the branches for a time tied to restoring the premises and the data: days, not hours.                                                                                                                                                                      |                              |
| WHAT WE RECOMMEND   | <b>Immediately</b> : smoke and flood detection with alarm; off-site copy of the data. <b>Within 6 months</b> : a secondary room, even a small one, in the building or elsewhere, with the essential services and an up-to-date copy. <b>Continuity plan</b> with declared recovery objectives. |                              |
| EFFORT AND PRIORITY | Short-term measures: low. Secondary room: medium-high. High priority (fix within 30 days for the short-term measures).                                                                                                                                                                         |                              |

# Level 7 · Intervention plan

CHAPTER 14 · PART B — THE SEVEN NETWORK ANALYSES

The last level puts in order what the previous six have found: **what to do first, what next, who does it and how much effort it takes**. It is a network improvement plan, broader in perspective than the one covering only the security findings (chapter 22, after the penetration test). The two plans are coordinated: some actions appear in both and are done only once.

## 14.1 The numbers of the seven analyses and of the test

| Part                                 | CRITICAL | HIGH | MEDIUM | LOW | INFO · STRENGTH | Total |
|--------------------------------------|----------|------|--------|-----|-----------------|-------|
| Level 1 · Discovery and inventory    | 0        | 1    | 1      | 1   | 1               | 4     |
| Level 2 · Topology and routing       | 0        | 0    | 1      | 2   | 2               | 5     |
| Level 3 · Performance and capacity   | 0        | 0    | 1      | 1   | 1               | 3     |
| Level 4 · Security and segmentation  | 0        | 1    | 2      | 1   | 2               | 6     |
| Level 5 · Configuration and updates  | 0        | 1    | 2      | 2   | 1               | 6     |
| Level 6 · Reliability and continuity | 0        | 2    | 2      | 1   | 1               | 6     |
| Seven analyses                       | 0        | 5    | 9      | 8   | 8               | 30    |
| Penetration test (chapter 20)        | 1        | 3    | 4      | 3   | 5               | 16    |
| Total                                | 1        | 8    | 13     | 11  | 13              | 46    |

Level 7 is this plan: it produces no findings of its own. The codes R1-... R6-... indicate the findings of the levels; PT-... those of the penetration test.

## 14.2 What to do, and when

| When             | Findings                      | Action                                                                                                                                    | Who                  | Effort |
|------------------|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|----------------------|--------|
| NOW · 72 HOURS   | PT-01 · R4-01                 | Change the credentials of the backup console; restrict management to two administration workstations.                                     | Technical contact    | Low    |
| NOW · 72 HOURS   | PT-03 · R5-01                 | Update the floor 4 switch; verify the versions of all floor devices; check the logs.                                                      | IT team              | Low    |
| NOW · 72 HOURS   | R1-01                         | Isolate the virtual machine with the unsupported system, pending a decision on whether to keep it.                                        | IT team              | Low    |
| WITHIN 30 DAYS   | PT-02 · PT-04 · R5-02         | Printer credentials; mail server updates with a monthly window.                                                                           | IT team              | Low    |
| WITHIN 30 DAYS   | R5-01                         | Update procedure that reports devices not reached; report for IT.                                                                         | IT team              | Medium |
| WITHIN 30 DAYS   | R6-02                         | Off-site copy of the backups, encrypted; immutable copy.                                                                                  | Technical contact    | Medium |
| WITHIN 30 DAYS   | R1-01 · R1-02                 | Decommission or update the virtual machine; assign an owner to each device not on the list.                                               | IT team              | Low    |
| WITHIN 90 DAYS   | PT-05 · PT-06 · PT-07 · PT-08 | VPN algorithms; guest Wi-Fi isolation; video recorder management; service accounts with expiry.                                           | IT team              | Medium |
| WITHIN 90 DAYS   | R2-01 · R3-01 · R5-03         | Spanning tree root fixed; firewall load test before July; personal accounts on the devices.                                               | IT team              | Medium |
| WITHIN 90 DAYS   | R4-02 · R4-03                 | Separate management network; start of device authentication on ports (first pilot floor).                                                 | IT team + consultant | High   |
| WITHIN 6 MONTHS  | R6-01 · R6-03                 | Smoke and flood detection; secondary room for essential services; second electrical line with separate UPS.                               | Sponsor + facilities | High   |
| WITHIN 6 MONTHS  | R5-04 · R5-05 · R3-02         | Secure SNMP management; central log archive; same voice priority on all floors.                                                           | IT team              | Medium |
| WITHIN 12 MONTHS | R2-02 · R6-04 · R6-05         | Traffic split between suppliers; critical points distributed between switches A and B; yearly failover tests and quarterly restore tests. | IT team              | Medium |

#### TO BE DECIDED · WHAT BRINGS THE MOST VALUE FIRST

The “Now” and “Within 30 days” actions cost a few hours and visibly reduce the risk: they protect the backups, the floor core and the public services. The architecture interventions (secondary room, management network, device authentication) have a larger effort and are best scheduled with a dedicated budget, after the 8 July check.

# External perimeter

CHAPTER 15 · PART C — THE PENETRATION TEST (EFESTO, ADVANCED LEVEL)

The penetration test starts from outside: **what anyone on the Internet can see and what they can try**. The aim is to know whether Voltaria's public addresses, the services in the DMZ and the branch VPNs hold up against a realistic attempt, without ever exceeding the kick-off limits. Activity of days G3 (observation from outside only) and G4 (edge, firewall and VPN, with read-only configuration checks).

BONET™ TOOLS AND ACTIVITIES · HOW WE WORK FROM OUTSIDE

Tests start from the external observation point (H4, a server in a data centre in Italy with a fixed address, agreed at the kick-off): Voltaria knows where they come from and can recognise them. Limited intensity, one test at a time, no saturation attempts. Every session starts and ends with a notice to the technical contact.

## 15.1 What was tested

| Area             | Scope and consent                                                                                         | What was done                                                                                         |
|------------------|-----------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Public addresses | Block 203.0.113.0/24; consent of the two suppliers (letters of 21 April).                                 | Discovery of reachable addresses, ports and services; comparison with the list of published services. |
| Mail and website | Mail and web servers in the DMZ.                                                                          | Check of versions, certificates, security settings and declared updates.                              |
| Branch VPNs      | Concentrator in the DMZ; <b>head-office side only</b> (the networks of the 40 branches are out of scope). | Check of algorithms, encryption parameters and access criteria.                                       |
| Edge (BGP)       | Edge routers; read-only.                                                                                  | Check of filters and route limits; no route announced or withdrawn.                                   |
| Firewall         | High-availability firewall pair.                                                                          | Comparison of the rules in force with the documentation; check of the zones.                          |
| DMZ              | Intermediate zone towards the internal network.                                                           | Check that public services do not reach internal networks beyond what is necessary.                   |

## 15.2 What emerged

| ID    | Severity   | Title                                                    | What it means                                                                                                                                                                                                                              |
|-------|------------|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PT-04 | HIGH       | Mail server in the DMZ with security updates behind      | Four months of fixes not applied on a service reachable from the Internet: whoever knows the missing fixes has a starting point. No exploitation was attempted on this service: the finding is based on the version and the missing fixes. |
| PT-05 | MEDIUM     | Branch VPNs with dated encryption algorithms             | The concentrator still accepts settings that are discouraged today, for compatibility with the old devices of some branches.                                                                                                               |
| PT-09 | LOW        | Web services revealing software name and version         | The information helps whoever looks for known weaknesses. Easy to hide.                                                                                                                                                                    |
| PT-12 | ✓ STRENGTH | BGP prefix filters correct                               | The edge accepts only what it should.                                                                                                                                                                                                      |
| PT-13 | ✓ STRENGTH | Firewall: rules documented and consistent with the zones | The observed behaviour matches the documentation.                                                                                                                                                                                          |
| PT-15 | ✓ STRENGTH | DMZ correctly separated from the internal network        | From the public services the users' networks cannot be reached.                                                                                                                                                                            |

NOTE · PUBLISHED SERVICES

Eleven services are reachable from the Internet: all on the list and all expected. No unexpected service, no administration interface exposed. This is a strength of the perimeter and supports the overall positive judgement in chapter 20.

**WHAT WAS NOT DONE**

No denial-of-service or saturation tests; no attempts to guess passwords on the published services; no change of BGP routes; no tests on the branch networks; no social engineering.

# Internal network and floors

CHAPTER 16 · PART C — THE PENETRATION TEST (EFESTO, ADVANCED LEVEL)

The second question is: **what can a device already inside the network do**, for example the computer of an employee, a guest or an external technician plugged into a socket. To answer, the test unit in the CED reaches six floor switches chosen by the client (T1–T6) over dedicated links, and from there we test, in a controlled way, what a device connected at that point would see. Activity of days G5 (from the CED), G6, G7 and G8 (floors, outside office hours).

## 16.1 The six points under test

| Point | Floor              | Day | Window     | Outcome                                          |
|-------|--------------------|-----|------------|--------------------------------------------------|
| T1    | Floor 1            | G6  | 20:30–2:00 | No anomalies beyond findings PT-10, PT-11        |
| T2    | Floor 2            | G6  | 20:30–2:00 | No anomalies beyond findings PT-10, PT-11        |
| T3    | Floor 3            | G7  | 20:30–2:00 | PT-01 (access to the backup network, chapter 18) |
| T4    | Floor 4            | G7  | 20:30–2:00 | <b>HIGH</b> PT-03 (switch behind in version)     |
| T5    | Floor 5 · switch A | G8  | 22:00–4:00 | Failover verified (PT-14)                        |
| T6    | Floor 5 · switch B | G8  | 22:00–4:00 | Failover verified (PT-14)                        |

For the floor 3 switch, which has no free fibre port, an adapter on an access port is used (feasibility study, chapter 6). The windows are those approved at the kick-off; in each one the BoNet™ project manager and an IT contact from Voltaria are present.

## 16.2 What emerged

| ID    | Severity          | Title                                                                                          | What it means                                                                                                                                                                                       |
|-------|-------------------|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PT-03 | <b>HIGH</b>       | Floor switch left without an update after maintenance: a workstation obtains unintended access | The weakness is not a faulty device but a step in the process: the periodic update did not reach a switch that was powered off for maintenance and no check reported it. Full record in chapter 20. |
| PT-10 | <b>LOW</b>        | Local name-resolution protocols active without need                                            | Name-lookup services that computers use when they do not find a name in the main systems: useful to few today, they can be abused to intercept requests.                                            |
| PT-11 | <b>LOW</b>        | IP phone web interface reachable from the data network                                         | The management page of each phone opens from the computers; without a strong password it could be misused.                                                                                          |
| PT-14 | <b>✓ STRENGTH</b> | Failover between switches A and B working as designed                                          | See below.                                                                                                                                                                                          |

## 16.3 The failover test on floor 5 (G8)

It is the highest-risk test of the internal part, which is why it takes place in a protected window (22:00–4:00), with the recovery plan already open, the BoNet™ project manager on site, the IT contact and the electrician on call. One of the two floor switches (A) was **shut down in an orderly way**, with the technical contact's consent, and we observed what happened to the connected devices; then the same was done with the other (B).

| What was observed                                                       | Result               |
|-------------------------------------------------------------------------|----------------------|
| Devices connected to both switches through a dual link remain reachable | <b>✓ AS DESIGNED</b> |

| What was observed                                                                                              | Result           |
|----------------------------------------------------------------------------------------------------------------|------------------|
| Switchover time of the links between the cores                                                                 | about 3 seconds  |
| IP phones and computers with a single link on the switch that was shut down lose the network until restoration | EXPECTED (R6-04) |
| Return to the initial state, with check of sessions, phones and printers                                       | ✓ SUCCESSFUL     |

RECOVERY · NO STOP

Day G8 ended without any stop condition being triggered. The last step was the check, with the IT contact, of the floor 5 devices when the offices reopened.

WHAT WAS NOT DONE

No change to the configurations of switches or cores; no test that saturates links; no reading of contents of computers, phones or printers; no tests outside the windows.

# Guest Wi-Fi, cameras, printers

CHAPTER 17 · PART C — THE PENETRATION TEST (EFESTO, ADVANCED LEVEL)

Guest Wi-Fi, cameras and printers have one thing in common: they are devices **that are easily forgotten**, often with factory settings. That is why they are tested together, on day G9, in reduced hours (Wi-Fi and printers by day, cameras in a window agreed with the physical security manager). No video footage and no document in a print queue was touched.

## 17.1 What was tested

| Area        | What was verified                                                                                                                 | Outcome              |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------|
| GUEST WI-FI | Separation of the guest network from the internal network; visibility between guest devices; acceptance page and access duration. | Separation OK; PT-06 |
| PRINTERS    | Administration interfaces on a sample of 60 printers on floors 1-5: credentials, active services, firmware.                       | PT-02                |
| CAMERAS     | Isolation of the camera network; management interfaces of the recorder and the cameras; paths towards the data network.           | PT-07                |

## 17.2 What emerged

| ID    | Severity | Title                                                                 | What it means                                                                                                                                                                                                        |
|-------|----------|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PT-02 | HIGH     | Printers with default administration credentials                      | On 14 printers out of 60 the manufacturer's credentials are still valid. Printers hold address books and, sometimes, documents: they are a foothold for whoever moves around the network. Full record in chapter 20. |
| PT-06 | MEDIUM   | Guest Wi-Fi with no isolation between connected devices               | Voltaria's internal network cannot be reached by guests, but guests can see each other. Record in chapter 20.                                                                                                        |
| PT-07 | MEDIUM   | The camera network reaches the data network through a management port | The video recorder has a second port on the data network. No video stream was opened: only the path was verified. It confirms finding R4-02.                                                                         |

✓ STRENGTHS

The guest network is separated from the internal network as designed. The cameras cannot be reached from the Internet and do not communicate with each other in an unintended way. The printers are on a dedicated network and respond only to the print servers and to users.

WHAT WAS NOT DONE

No viewing of footage or printed documents; no change of printer or camera settings (the default credentials were verified only with a brief access, closed at once, on two printers chosen by IT); no tests intercepting other guests on the Wi-Fi.

# Services and backup

CHAPTER 18 · PART C — THE PENETRATION TEST (EFESTO, ADVANCED LEVEL)

This is the part that matters most to the business owner: **the services everyone's work depends on** (mail, files, the user directory, business applications) and **the backup copies** from which operations would restart after a failure or an attack. Activity of day G10, during working hours, changing nothing, with the technical contact present. Chapter 13 had already shown the limits of continuity; here we see whether, from inside the network, the copies are truly safe.

## 18.1 What was verified

| Area                  | What was verified                                                                                                                            | Outcome                |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| User directory        | Health of the user and group list; service accounts; password policies; privilege paths.                                                     | PT-08                  |
| Mail and files        | Access controls on internal services and shares; exposure from inside.                                                                       | No additional findings |
| Business applications | Access to portals and database services, only the authentication part; no reading of data.                                                   | No additional findings |
| Backup system         | Reachability of the administration console from the users' network; credentials; state of the copies; isolation from the production network. | PT-01                  |

## 18.2 What emerged

| ID    | Severity | Title                                                                         | What it means                                                                                                                                                                                                                                    |
|-------|----------|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PT-01 | CRITICAL | Backup system console reachable from the users' network with weak credentials | Whoever reached that console could delete or alter the backup copies. It is the only critical finding, and it is so because it puts at risk the ability to restart after an incident. Full record in chapter 20; controlled proof in chapter 19. |
| PT-08 | MEDIUM   | Directory service account with a password that never expires                  | Accounts used by programs and not by people, with passwords unchanged for years: if the password were discovered, the access would remain valid for a long time.                                                                                 |

## 18.3 The state of the copies

The **restore test of 20–21 April**, carried out by Voltaria as a preliminary condition of the engagement, succeeded: the data of the last copy were restored in a separate environment. The previous test dated back fourteen months (finding R6-02). All the copies are in the data centre and none is immutable: that is why the backup console reachable by users (PT-01) is critical.

RECOVERY · BACKUP FIRST

Day G10 was subject to the successful restore test (condition 1 of the study). Had the test failed, the test would not have started: no invasive engagement begins without knowing that restoration is possible.

WHAT WAS NOT DONE

No reading of mailboxes, documents or business application data; no change or deletion of backup copies; no attempt to guess passwords on directory accounts; no restoration from production data during the test.

# Controlled exploitation and impact check

## CHAPTER 19 · PART C — THE PENETRATION TEST (EFESTO, ADVANCED LEVEL)

Some findings can be demonstrated only by testing up to a certain point what would really happen. It is the most delicate part of the engagement: that is why it takes place on day G11, **one test at a time**, only for points already identified on the previous days, with the written consent of the technical contact for each one and with the BoNet™ project manager on site. The aim is not to “get in”: it is to **measure the impact with the smallest possible test**, and then stop.

### BONET™ TOOLS AND ACTIVITIES · THE TOOLS OF THIS DAY

The tools for these tests are not listed in chapter 5: they are chosen case by case and agreed at the kick-off, one test at a time. None of them is used outside the approved window and scope.

## 19.1 The three tests of the day

| Test | Finding                     | What was demonstrated                                                                                                                               | What was not touched                                     |
|------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| 1    | <b>PT-01</b> Backup console | Access to the console with a credential deducible from lists of widespread passwords, from the floor 3 access port. Access closed at once.          | No copy read, changed or deleted; no setting changed.    |
| 2    | <b>PT-03</b> Floor 4 switch | From point T4, a connected workstation reached a network different from the one assigned, towards a test system indicated by the technical contact. | No other system; no data read; no configuration changed. |
| 3    | <b>PT-02</b> Printers       | Access to the administration interface of two printers chosen by IT, with the manufacturer's default credential. Access closed at once.             | No document, no address book read; no setting changed.   |

## 19.2 How each test is carried out

1. **Consent.** The technical contact signs, on a dedicated form, the test about to begin: point, finding, window, what will be touched and what will not.
2. **Recovery plan open.** The scenario of the test and who steps in are re-read.
3. **Minimal test.** The finding is demonstrated with the bare minimum; no data is read or copied, no change remains.
4. **Evidence.** Date, time, operator and fingerprint (SHA-256) in the evidence log; no personal content.
5. **Stop and check.** Access is closed, everything is verified to be as before and the closing of the test is signed.

### ✓ OUTCOME OF THE DAY

No stop condition triggered; no service showed anomalies; no alarm from Voltaria's monitoring system. The internal IT **did not detect** tests 1 and 3: this is useful information, because it indicates that monitoring of access to consoles and printers can be improved (recommendation in the remediation plan).

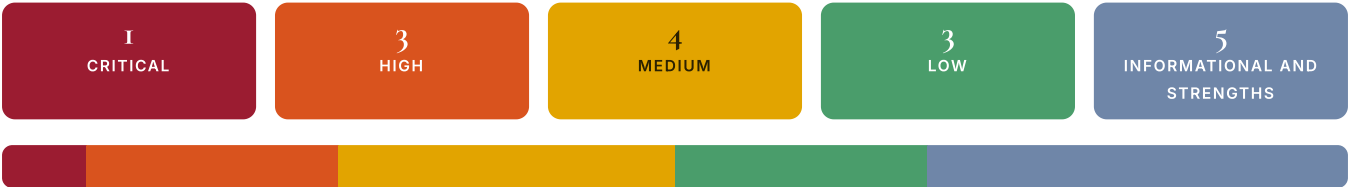
### WHAT WAS NEVER DONE

No denial-of-service tests; no persistent access left on the systems; no change or deletion of the client's data; no exfiltration of content; no tests outside the approved scope; no attempt to evade Voltaria's monitoring.

# Penetration test findings

CHAPTER 20 · PART C — EFESTO, ADVANCED LEVEL

The penetration test tried, in a controlled and authorised way, whether the weaknesses identified could really be exploited, and what would follow. The result is positive on the perimeter (firewall, BGP, DMZ and network separation are well set up) and shows few points to act on with priority, almost all **inside** the network; one concerns a **procedure** (the update of floor switches) more than a single device. All findings were tested without reading or changing the client's data.



## 20.1 Summary

| ID    | Severity      | Title                                                                                          | Where                | Record        |
|-------|---------------|------------------------------------------------------------------------------------------------|----------------------|---------------|
| PT-01 | CRITICAL      | Backup system console reachable from the users' network with weak credentials                  | CED · users' network | § 20.2        |
| PT-02 | HIGH          | Printers with default administration credentials                                               | Floors 1–5           | § 20.2        |
| PT-03 | HIGH          | Floor switch left without an update after maintenance: a workstation obtains unintended access | Floor 4 · T4         | § 20.2        |
| PT-04 | HIGH          | Mail server in the DMZ with security updates behind                                            | DMZ                  | Full document |
| PT-05 | MEDIUM        | Branch VPNs with dated encryption algorithms                                                   | Firewall             | Full document |
| PT-06 | MEDIUM        | Guest Wi-Fi network with no isolation between connected devices                                | Ground floor         | § 20.2        |
| PT-07 | MEDIUM        | The camera network reaches the data network through a management port                          | CED                  | Full document |
| PT-08 | MEDIUM        | Directory service account with a password that never expires                                   | CED · directory      | Full document |
| PT-09 | LOW           | Web services in the DMZ reveal software name and version                                       | DMZ                  | Full document |
| PT-10 | LOW           | Local name-resolution protocols active without need                                            | Users' network       | Full document |
| PT-11 | LOW           | IP phone web interface reachable from the data network                                         | Floors 1–5           | Full document |
| PT-12 | ✓ STRENGTH    | Edge routers: BGP prefix filters correct                                                       | Edge                 | Full document |
| PT-13 | ✓ STRENGTH    | Firewall: rules documented and consistent with the zones                                       | Firewall             | Full document |
| PT-14 | ✓ STRENGTH    | Failover between switches A and B working as designed (G8)                                     | Floor 5              | Full document |
| PT-15 | ✓ STRENGTH    | DMZ correctly separated from the internal network                                              | DMZ                  | Full document |
| PT-16 | INFORMATIONAL | REI120 risers and passages: no anomaly found                                                   | Risers               | Full document |

## 20.2 Four records as an example

|                   |                                                                                                                                                                                                                                          |                                                                               |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| PT-01             | CRITICAL                                                                                                                                                                                                                                 | <b>Backup console reachable from the users' network with weak credentials</b> |
| WHERE             | Backup system in the CED; test performed from the floor 3 access port (point T3), day G7/G10.                                                                                                                                            |                                                                               |
| WHAT WE OBSERVED  | The administration interface of the backup system is reachable from any computer on the users' network. The administration credentials turned out to be among the most common ones.                                                      |                                                                               |
| PROOF             | Access to the console achieved with a credential deducible from lists of widespread passwords. <b>No data was read or changed</b> ; the access was closed at once. Evidence EV-031, with date, time and fingerprint in the evidence log. |                                                                               |
| IMPACT            | Whoever obtained this access could delete or alter the backup copies. Together with finding R6-02, recovery after an attack or a failure would be at risk.                                                                               |                                                                               |
| WHAT WE RECOMMEND | <b>Immediately (within 72 hours):</b> change the credentials; restrict access to the console to two administration workstations. <b>Within 30 days:</b> multi-factor authentication; separate management network; immutable copy.        |                                                                               |
| FOLLOW-UP CHECK   | Repeat of the test at 30 days (8 July 2026).                                                                                                                                                                                             |                                                                               |

|                   |                                                                                                                                          |                                                         |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| PT-02             | HIGH                                                                                                                                     | <b>Printers with default administration credentials</b> |
| WHERE             | Printer network, floors 1–5; test from points T1–T6.                                                                                     |                                                         |
| WHAT WE OBSERVED  | On 14 of the 60 printers the administration interface accepts the credentials supplied by the manufacturer.                              |                                                         |
| IMPACT            | Printers hold documents and address books, and are often a foothold for whoever tries to move around the network.                        |                                                         |
| WHAT WE RECOMMEND | Change the credentials on all printers; disable unused services; update the firmware; restrict administration access to one workstation. |                                                         |
| EFFORT            | Low (a few hours). High priority: fix within 30 days.                                                                                    |                                                         |

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                       |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| PT-03             | HIGH                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <b>Floor switch left without an update after maintenance: a workstation obtains unintended access</b> |
| WHERE             | Floor 4 switch (point T4); day G7. Emerged from the comparison of the switches' software versions (level 5 inventory) and confirmed with a test from point T4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                       |
| WHAT WE OBSERVED  | Floor switches are updated periodically by the internal IT with a scheduled procedure. The floor 4 switch turned out to be <b>one security version behind</b> the other eleven: it was powered off for maintenance during the window of the last update and the procedure did not report that this device had not been reached, nor did it pick it up when it came back into service. On that device a workstation connected to an access port was able to reach networks other than the one assigned, because of an <b>access-control problem whose precise cause we have not identified</b> (the most likely hypothesis is the missing fix contained in the next version: to be confirmed with the manufacturer). |                                                                                                       |
| PROOF             | From point T4, in the agreed window, it was verified that the intended separation between the users' network and the other networks was not respected, reaching only a test system indicated by the technical contact. <b>No data was read or changed</b> . Evidence EV-044, with date, time and fingerprint in the evidence log.                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                       |
| IMPACT            | A compromised workstation, or simply one connected to that switch, could reach networks and systems that are not its concern. The weakness is not an isolated fault but <b>a step in the process</b> : no check reports the devices left behind, and the same could happen with any switch that is off or unreachable during an update.                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                       |
| WHAT WE RECOMMEND | <b>Immediately (within 72 hours):</b> update the floor 4 switch; verify the version of all floor devices; check the logs for unusual access from that floor's workstations. <b>Within 30 days:</b> have the procedure report the devices not reached, with automatic retries and a report for IT; automatic comparison of versions with the reference one; device authentication on the access ports. <b>Within 90 days:</b> quarterly check of versions, recorded.                                                                                                                                                                                                                                                 |                                                                                                       |
| EFFORT            | Low for the update (a few hours); medium for correcting the procedure. High priority.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                       |
| FOLLOW-UP CHECK   | Repeat of the test at 30 days (8 July 2026).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                       |

|                                                                                     |                                                                                                                                                  |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| PT-06 <b>MEDIUM</b> Guest Wi-Fi network with no isolation between connected devices |                                                                                                                                                  |
| WHERE                                                                               | Ground-floor waiting room, day G9.                                                                                                               |
| WHAT WE OBSERVED                                                                    | The guest network is separated from the internal network, as intended. Devices connected to the same guest network, however, can see each other. |
| IMPACT                                                                              | A visitor could observe or disturb another visitor's devices. Voltaria's internal network cannot be reached.                                     |
| WHAT WE RECOMMEND                                                                   | Enable client isolation on the access point; acceptance page with access expiry; per-guest bandwidth limit.                                      |
| EFFORT                                                                              | Low (a setting). Medium priority: fix within 90 days.                                                                                            |

# Clean-up and restoration

CHAPTER 21 · PART C — THE PENETRATION TEST (EFESTO, ADVANCED LEVEL)

The last test day (G12) produces no findings: **it puts everything back as it was**. Everything created by the tests is removed, the routes and spaces are returned, it is verified that the network is identical to how it was before, and the engagement on the ground is closed with a meeting and signed minutes. Present: BoNet™ project manager, support technician, Voltaria's technical contact and facilities manager, electrician, cabler, sponsor for the closing meeting.

## 21.1 What was done

| Area                      | Action                                                                                                                                                    | Check                                               |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| Test hardware             | Orderly shutdown and removal of the test unit (H1), the optical aggregator (H2), the dedicated UPS, the optical modules and the cables from the CED rack. | Photos of the rack before and after; signed minutes |
| Power and cooling         | Disconnection from the dedicated line; final readings of power draw and temperature.                                                                      | Values compared with the initial survey             |
| Routes to the floors      | Return of the spare routes with a continuity test (cabler); no fibre left connected.                                                                      | Route certificates; minutes                         |
| Accesses and accounts     | Revocation of every account, key and credential created for the tests; closing of the emergency access (LTE) and of the SIM.                              | List signed by the technical contact                |
| Voltaria's configurations | Comparison with the configuration copies taken at the kick-off: no change in the cores, switches, firewalls and routers.                                  | Fingerprints compared; outcome: no differences      |
| Evidence                  | Closing of the evidence log with a final fingerprint; encrypted copy to the BoNet™ archive; secure erasure of the test devices within 30 days.            | Log (appendix B); erasure certificate               |
| Passages in the risers    | No opening made: only existing passages were used. Check by the cabler and the facility manager.                                                          | Anomalies: none (informational finding PT-16)       |

## 21.2 Before and after

| Measurement in the CED                                     | Initial survey (G1) | After removal (G12)        |
|------------------------------------------------------------|---------------------|----------------------------|
| Air temperature at the rack intake                         | 22.1 °C             | 22.2 °C                    |
| Power draw of the dedicated line                           | 0 W                 | 0 W (disconnected)         |
| Peak power draw during the tests (unit + aggregator + UPS) | —                   | 187 W (peak), 64 W average |
| Differences in Voltaria's configurations                   | —                   | None                       |
| Accounts and credentials of the tests                      | —                   | All revoked                |

RECOVERY · CHECK OF THE RETURN TO THE INITIAL STATE

Before leaving the data centre, the technical contact checks, together with BoNet™, the state of the critical services (mail, business applications, branch VPNs, backup) and the absence of alarms. Only then are the **restoration minutes** signed, which go into the handover (chapter 23).

TO BE DECIDED · AFTER CLOSURE

The 30-day follow-up check (chapter 24) does not require reinstalling the hardware in the CED: the mobile unit is used, unless otherwise agreed. A new installation is agreed case by case.

# Remediation plan

## CHAPTER 22 · PART C — THE PENETRATION TEST (EFESTO, ADVANCED LEVEL)

A finding that is not fixed is a problem postponed. The remediation plan turns the penetration test findings into **actions with an owner, a deadline and a verification test** (request R9). Fixes are the client's activity: BoNet™ proposes and verifies, it does not change the systems. The plan is coordinated with that of chapter 14: actions that appear in both are done once.

### 22.1 The actions, finding by finding

| ID    | Severity | Action                                                                                                                                                     | When                         | Who                         | Verification test                                         |
|-------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|-----------------------------|-----------------------------------------------------------|
| PT-01 | CRITICAL | Change the credentials; restrict the console to two administration workstations; multi-factor authentication; separate management network; immutable copy. | 72 hours (measures); 30 days | Technical contact           | Repeat of the test from point T3: access must not succeed |
| PT-02 | HIGH     | Change the credentials on all printers; disable unused services; update the firmware.                                                                      | 30 days                      | IT team                     | Check on all 62 printers                                  |
| PT-03 | HIGH     | Update the floor 4 switch; automatic report of devices not reached; device authentication on ports (pilot).                                                | 72 hours; 30 days; 90 days   | IT team                     | Versions of all switches; separation test from point T4   |
| PT-04 | HIGH     | Apply the updates that are behind; monthly window.                                                                                                         | 30 days                      | IT team                     | Version and fixes verified from outside                   |
| PT-05 | MEDIUM   | Disable the dated algorithms; update the branches with old devices.                                                                                        | 90 days                      | IT team + branches          | Check of the concentrator; list of branches migrated      |
| PT-06 | MEDIUM   | Client isolation on guest Wi-Fi; access expiry; bandwidth limit.                                                                                           | 90 days                      | IT team                     | Test from the waiting room                                |
| PT-07 | MEDIUM   | Move the recorder's management to the management network; explicit rule between networks.                                                                  | 90 days                      | IT team + physical security | Path test between the two networks                        |
| PT-08 | MEDIUM   | Service accounts with a long password and expiry; inventory of service accounts.                                                                           | 90 days                      | IT team                     | Directory check                                           |
| PT-09 | LOW      | Hide software name and version in the web services.                                                                                                        | Scheduled intervention       | IT team                     | Check from outside                                        |
| PT-10 | LOW      | Disable the unnecessary local name-lookup protocols.                                                                                                       | Scheduled intervention       | IT team                     | Check from points T1-T6                                   |
| PT-11 | LOW      | Restrict access to the phones' web page to the management network; strong password.                                                                        | Scheduled intervention       | IT team                     | Check from points T1-T6                                   |

Findings PT-12–PT-16 are strengths or informational: no action, but they must be maintained over time. The actions on the findings of the levels (R1–... R6–...) are in chapter 14.

### 22.2 A suggestion on monitoring

#### TO BE DECIDED · SEEING WHAT HAPPENS

On day G11 Voltaria's monitoring system did not report the access to the backup console or to the printers. We recommend enabling alerts on administrative access to consoles, new devices on access ports and changes of device versions: they do not prevent an incident, but they let you notice it in minutes and not in weeks.

### 22.3 The recommended order

1. **Protect the backups** (PT-01): it is what operations restart from after an incident.
2. **Close the floor weakness** (PT-03): update and control of versions.
3. **Close the doors open from outside** (PT-04, PT-05).
4. **Fix the forgotten devices** (PT-02, PT-06, PT-07).
5. **Schedule the underlying fixes** (management network, device authentication, log archive).

# Handover: delivery and transfer

CHAPTER 23 · PART C — CLOSING THE ENGAGEMENT

The handover is the moment when BoNet™ **returns everything to Voltaria** and passes the knowledge to the internal team: documents, evidence, hardware, accesses and responsibilities. It is not a formality. This is where we verify that what feasibility study SF-2026-014 had promised, and what the kick-off of 28 April had signed, has really been delivered. The handover takes place on **10 June 2026**, two days after the delivery of the report.

## 23.1 What is delivered

| Document or asset             | Contents                                                                                                                 | To whom                            |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| Complete report               | The seven analyses, the penetration test, findings by severity, the remediation plan; in Italian and in English, signed. | Sponsor, technical contact         |
| Summary attestation           | Two pages, without sensitive details, to show to clients and the insurer (request R7).                                   | Sponsor                            |
| Evidence log                  | Every test with date, time, operator and SHA-256 fingerprint, on encrypted media.                                        | Technical contact, privacy officer |
| Updated inventory and diagram | The network as it is, with the differences from Voltaria's documents listed and corrected (request R4).                  | Technical contact                  |
| Remediation plan              | Interventions in priority order, with times, proposed owners and verification test (request R9).                         | Sponsor, technical contact         |
| Cabling dossier               | Routes used, certifications, restoration of the passages in the REI120 risers, signed by the cabler.                     | Facilities manager                 |
| Restoration minutes (G12)     | Return to the initial state, with temperature and power readings, photos and signatures.                                 | Facilities manager                 |
| List of tools and licences    | Versions and licence types used (appendix A).                                                                            | Sponsor                            |
| Study and kick-off minutes    | Study SF-2026-014 and the minutes of 28 April, updated with what changed during the engagement.                          | Sponsor                            |

## 23.2 Transfer to the IT team

The workshop is half a day, on 10 June 2026, with the two internal technicians, the sponsor and the privacy officer. It serves to ensure that the results stay in Voltaria's hands (request R10).

| Time        | Topic                                                                               | Participants                                |
|-------------|-------------------------------------------------------------------------------------|---------------------------------------------|
| 9:00–10:00  | Summary for management: what emerged, what matters most.                            | Sponsor, technical contact, privacy officer |
| 10:00–11:30 | The findings one by one, with the evidence: from critical to low.                   | IT team, technical contact                  |
| 11:30–12:30 | The remediation plan: owners and deadlines are assigned.                            | Sponsor, technical contact, IT team         |
| 12:30–13:00 | How to repeat the failover tests and the periodic checks; proposed yearly calendar. | IT team                                     |

## 23.3 Closure and return

### What is returned or restored

- The test hardware is **removed from the CED** (G12) and the configurations go back to how they were.
- The **spare routes** are returned with minutes and a continuity test.
- The credentials and accesses created for the tests are **revoked**.
- The client's devices have undergone no changes.

### What is kept or destroyed

- The data on the test devices are **securely erased** within 30 days of closure.
- An encrypted copy of the evidence is **kept for 12 months**, for the follow-up check and for any disputes, then destroyed with a certificate.
- Access to the archive is only on written request of the technical contact.
- The licences remain BoNet™'s.

### 23.4 Traceability matrix

Every request of the feasibility study has its **outcome**, with the chapter of the report that deals with it. The outcome says whether the request has received an answer; fixing the weaknesses found is a separate activity, in the remediation plan.

| ID  | Request (study SF-2026-014)                          | Where it is covered              | Outcome                                |
|-----|------------------------------------------------------|----------------------------------|----------------------------------------|
| R1  | Fault tolerance without halting orders               | Ch. 13 · G8 · PT-14              | ✓ MET                                  |
| R2  | Exposure from the Internet                           | Ch. 15 · PT-04, PT-05, PT-09     | ✓ MET                                  |
| R3  | Compromised device on the floors or from guest Wi-Fi | Ch. 16-17 · T1-T6 · PT-03, PT-06 | ✓ MET                                  |
| R4  | Up-to-date, verified inventory                       | Ch. 8-9 · attachment             | ✓ MET                                  |
| R5  | Secure branch VPNs                                   | Ch. 15 · PT-05                   | 🕒 WITH RESERVATION<br>head-office side |
| R6  | State of backups and restoration                     | Ch. 13 · ch. 18 · PT-01          | ? TO BE VERIFIED<br>after the fix      |
| R7  | Report and attestation for clients and the insurer   | Ch. 23.1                         | ✓ MET                                  |
| R8  | No halt to orders                                    | Ch. 4 · ch. 6                    | ✓ MET                                  |
| R9  | Remediation plan and verification                    | Ch. 22 · ch. 24                  | ? TO BE VERIFIED on 8 July             |
| R10 | Knowledge transfer                                   | Ch. 23.2                         | ✓ MET                                  |
| R11 | Confidentiality and personal data                    | Ch. 4 · ch. 23.3                 | ✓ MET                                  |

**In summary:** 8 requests met, 1 with reservation (the branches' networks were out of scope), 2 to be verified after the fix. The check of 8 July (chapter 24) closes them.

**BONET™ TOOLS AND ACTIVITIES · AFTER DELIVERY**

For thirty days from delivery, clarifications on the report are included in the engagement. Mandate VD-2026-031 closes with the **delivery minutes**, signed by Voltaria's sponsor and the BoNet™ project manager; the thirty-day check is a separate activity, already provided for by the feasibility study.

For Voltaria Distribuzione S.p.A. — General manager  
Date and signature

For BoNet™ — Project manager  
Date and signature

# 30-day follow-up check

CHAPTER 24 · PART C — CLOSING THE ENGAGEMENT

The Advanced level includes a **follow-up check after thirty days**: the tests are repeated on the points Voltaria has declared corrected, to check that the fix really works. On 8 July 2026 the check took place in half a day, with the mobile unit and the technical contact present, without reinstalling the hardware in the CED. This chapter is an update of the report, in the same format.

## 24.1 Outcome by finding

| ID              | Initial severity | What Voltaria did                                                                                                             | Outcome of the check              |
|-----------------|------------------|-------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| PT-01           | CRITICAL         | Credentials changed; console restricted to two workstations; multi-factor authentication enabled; immutable copy in progress. | ✓ CLOSED (off-site copies remain) |
| PT-02           | HIGH             | Credentials changed on 60 printers out of 62; two old models being replaced.                                                  | ⦿ PARTIAL (2 open)                |
| PT-03           | HIGH             | Floor 4 switch updated; the procedure now produces a report of devices not reached and retries; monthly check of versions.    | ✓ CLOSED                          |
| PT-04           | HIGH             | Updates applied; monthly window agreed.                                                                                       | ✓ CLOSED                          |
| PT-05           | MEDIUM           | Dated algorithms disabled on 31 branches out of 40; the others being updated.                                                 | ⦿ PARTIAL (9 branches)            |
| PT-06           | MEDIUM           | Client isolation enabled.                                                                                                     | ✓ CLOSED                          |
| PT-07 ... PT-11 | MEDIUM · LOW     | In the 90-day intervention programmes or at the next scheduled intervention.                                                  | ? IN PROGRESS                     |

## 24.2 The requests that were “to be verified”

| ID | Request                           | Updated outcome                                                                    |
|----|-----------------------------------|------------------------------------------------------------------------------------|
| R6 | State of backups and restoration  | ✓ MET restore test repeated on 7 July; immutable copy active                       |
| R9 | Remediation plan and verification | ✓ MET with four findings closed and two partial                                    |
| R5 | Secure branch VPNs                | ⦿ WITH RESERVATION head-office side improved; the branch side remains out of scope |

✓ OVERALL OUTCOME

Six findings out of eleven are closed or being closed with a repeated test. The two most important points (backup and floor switches) are closed. For the architecture interventions (management network, secondary room, device authentication) a review in six months is proposed.

NOTE · HOW TO READ THE DATES

The document describes a fictitious engagement, with invented dates: the check “of 8 July” is a way of showing how the circle is closed.

# Appendix A · Tool licences

APPENDICES · LIST PRESENTED AT THE KICK-OFF OF 28 APRIL 2026

Every tool used in the engagement is listed with the type of licence and the version, **frozen at the kick-off**: results remain repeatable until closure. Commercial licences are purchased for the engagement and **registered in BoNet™'s name, not the client's**. In a real engagement the table carries real numbers and expiry dates: here the values are examples.

## A.1 Free software

| Tool                         | Function                         | Licence                                      | Version                                                                     |
|------------------------------|----------------------------------|----------------------------------------------|-----------------------------------------------------------------------------|
| Kali Linux                   | Base system                      | Free software (various licences, mostly GPL) | Rolling release of April 2026; image verified with the producer's signature |
| Nmap                         | Inventory and scanning           | Nmap Public Source License                   | Recorded at the kick-off                                                    |
| Greenbone Community Edition  | Vulnerability assessment         | GPL                                          | Recorded at the kick-off; vulnerability data updated to the same date       |
| Wireshark · Zeek · Suricata  | Traffic analysis                 | GPLv2 · BSD · GPLv2                          | Recorded at the kick-off                                                    |
| testssl.sh                   | Strength of encryption           | GPLv2                                        | Recorded at the kick-off                                                    |
| Kismet                       | Wi-Fi                            | GPLv2                                        | Recorded at the kick-off                                                    |
| iperf3                       | Performance                      | BSD                                          | Recorded at the kick-off                                                    |
| BloodHound Community Edition | Privilege paths in the directory | Apache 2.0                                   | Recorded at the kick-off                                                    |

## A.2 Commercial licences

| Tool                                  | Licence type                     | Number (example) | Expiry (example) | Registered to |
|---------------------------------------|----------------------------------|------------------|------------------|---------------|
| Tenable Nessus Professional           | Annual subscription per scanner  | EXAMPLE-0001     | 31 December 2026 | BoNet™        |
| Burp Suite Professional (PortSwigger) | Annual subscription per user     | EXAMPLE-0002     | 31 December 2026 | BoNet™        |
| PingCastle (Netwrix), for consultants | Commercial for service providers | EXAMPLE-0003     | 31 December 2026 | BoNet™        |

TO CHECK IN A REAL ENGAGEMENT

The terms of use of each tool (in particular the commercial ones) must be re-read before the engagement: they may limit use on third-party systems, the number of addresses or the delivery of results to the client.

## A.3 Test hardware

The models are in chapter 5. At the end, the disks of all units were securely erased (certificate in the evidence log) and the units returned to BoNet™'s stock.

# Appendix B · Evidence log

APPENDICES · AN EXTRACT OF THE LOG, AS AN EXAMPLE

Every test has a number (EV-xxx), a date and time, an operator and a **fingerprint (SHA-256)** of the evidence file: if the file is modified, the fingerprint changes. The log is kept on encrypted media and delivered to Voltaria at the handover; in the finding records only the number appears. The fingerprints here are shortened and invented. People's names do not appear: only the role.

| EV     | Date · time    | Day | Operator           | What it documents                                                                 | Fingerprint |
|--------|----------------|-----|--------------------|-----------------------------------------------------------------------------------|-------------|
| EV-004 | 12 May · 09:40 | G2  | Support technician | List of devices detected (passive inventory, 7 days)                              | a3f9...c07e |
| EV-012 | 13 May · 11:15 | G3  | Project manager    | Services reachable from the Internet (11), from external point H4                 | 71be...09d2 |
| EV-019 | 14 May · 15:02 | G4  | Project manager    | BGP filters and limits on the edge routers (read-only)                            | e45c...2a19 |
| EV-027 | 18 May · 22:30 | G6  | Project manager    | Visibility between networks from points T1 and T2                                 | 0d88...f3a4 |
| EV-031 | 19 May · 21:12 | G7  | Project manager    | Access to the backup console from point T3 (closed at once)                       | c2b0...58ee |
| EV-044 | 19 May · 23:48 | G7  | Project manager    | Separation between networks from point T4: software version of the floor 4 switch | 94ac...d1b7 |
| EV-053 | 20 May · 00:25 | G8  | Support technician | Floor 5 failover test: switchover and return times                                | 6f10...ab33 |
| EV-061 | 21 May · 10:50 | G9  | Support technician | Printers: 14 interfaces with default credentials                                  | 38d5...7e90 |
| EV-072 | 22 May · 14:05 | G10 | Project manager    | State of the directory: service accounts with no expiry                           | b71e...0c25 |
| EV-086 | 25 May · 23:10 | G11 | Project manager    | Controlled test no. 2 (floor 4 switch): signed consent and closing                | 1ee9...44f8 |
| EV-098 | 26 May · 16:30 | G12 | Project manager    | Restoration minutes: final readings, comparison of configurations                 | cd04...a6b2 |

#### NOTE · HOW THE LOG IS USED

If a finding is challenged, or if a year later one wants to repeat a test, the log makes it possible to know exactly what was done, when and by whom, and to check that the evidence has not been altered. The evidence is kept encrypted for twelve months and then destroyed, with a certificate (chapter 23.3).

# Appendix C · Glossary

## APPENDICES · THE WORDS USED, IN PLAIN LANGUAGE

| Term                                    | What it means                                                                                                                                    |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>802.1X</b>                           | A rule whereby a device must identify itself before obtaining a network from a socket or from Wi-Fi.                                             |
| <b>High availability</b>                | Two identical devices, one of which takes over if the other stops.                                                                               |
| <b>BGP</b>                              | The system by which a company with several Internet suppliers announces its own addresses: if one line drops, traffic passes through the others. |
| <b>CED</b>                              | Data centre (centro elaborazione dati): the room of the main servers and devices.                                                                |
| <b>Core</b>                             | The central device of the internal network, to which the floor switches connect.                                                                 |
| <b>DMZ</b>                              | A separate zone of the network where the services reachable from the Internet sit (mail, website, VPN), distinct from the internal network.      |
| <b>Evidence</b>                         | The proof of what was done: a file with date, time and fingerprint.                                                                              |
| <b>Failover</b>                         | The automatic switch from the main device to the spare one.                                                                                      |
| <b>Firewall</b>                         | A device that decides which communications are allowed between the zones of the network.                                                         |
| <b>Firmware</b>                         | The software built into a device (switch, printer, phone).                                                                                       |
| <b>Grey box · black box · white box</b> | How much information the test starts with: an ordinary account, no information, documentation and dedicated access.                              |
| <b>Handover</b>                         | The final delivery, with the transfer of knowledge to the client's team.                                                                         |
| <b>Fingerprint (SHA-256)</b>            | A code calculated from a file's content: if the file changes, the code changes.                                                                  |
| <b>Kick-off</b>                         | The initial meeting in which roles, limits, stop conditions and recovery are set.                                                                |
| <b>Penetration test</b>                 | An authorised and controlled test that checks whether weaknesses can really be exploited.                                                        |
| <b>Scope</b>                            | The set of addresses, devices and days authorised: what is not written stays out.                                                                |
| <b>Recovery</b>                         | What is done to return to normal after an interruption.                                                                                          |
| <b>REI120</b>                           | Fire-resistance class: the compartment holds for 120 minutes.                                                                                    |
| <b>Finding</b>                          | A weakness or good practice that emerged from the analysis, with severity, evidence and recommended fix.                                         |
| <b>SNMP</b>                             | Protocol by which devices provide monitoring data.                                                                                               |
| <b>Spanning tree</b>                    | A mechanism that avoids "loops" in the network between switches connected in more than one way.                                                  |
| <b>Spare (routes)</b>                   | Backup links already laid, used only in case of failure.                                                                                         |
| <b>Switch</b>                           | A device that connects the computers, phones and printers of a floor to one another.                                                             |
| <b>TAP</b>                              | A passive device that allows traffic to be observed without interrupting it.                                                                     |
| <b>VLAN</b>                             | A logical division of a physical network into separate networks (users, voice, printers...).                                                     |
| <b>VPN</b>                              | An encrypted tunnel to connect a distant site to the company network.                                                                            |

# Appendix D · Legal aspects

APPENDICES · WHAT MUST BE CLEAR IN WRITING BEFORE STARTING

An invasive test makes sense only if all parties know what happens, on what and with which responsibilities. This appendix summarises in simple form the points that the signed engagement defines. **It is not legal advice:** the text of mandate VD-2026-031 and of its technical annex prevails.

| Topic                           | What the engagement provides                                                                                                                                                                                                                                                                              |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Written authorisation           | Accessing a computer system without authorisation is a crime (art. 615-ter of the Italian Criminal Code). That is why no activity started before the mandate was signed by the controller together with its technical annex; the authorisation of the network analysis does not extend to invasive tests. |
| Scope, time, duration           | The authorisation applies only to the addresses, sites, devices, types of test, approaches, time windows and duration indicated. What is not written is excluded; any extension requires a new written agreement.                                                                                         |
| Third parties                   | For the lines of the two suppliers the written consent of each was needed (letters of 21 April 2026). Without consent, those systems stay out.                                                                                                                                                            |
| Risks and responsibility        | Voltaria was informed in writing that tests can cause slowdowns, malfunctions or interruptions, and confirmed that it has a verified backup (restore test of 20–21 April). The allocation of responsibilities and the limits are in the mandate.                                                          |
| Insurance                       | Insurance is at Voltaria's expense, as per the mandate. Voltaria informed its insurer in writing of the testing activity and kept the reply.                                                                                                                                                              |
| Personal data                   | The test neither looks for nor keeps content. Where personal data emerge, BoNet™ acts as data processor with a specific appointment (art. 28 of the GDPR), limits itself to the minimum test and destroys the evidence within the terms of the engagement, with an attestation on request.                |
| Compromises already in progress | If an incident already under way emerges, activities are suspended and the contact is informed at once; the notifications required by law, for example to the data protection authority, are the controller's responsibility.                                                                             |
| Confidentiality                 | Information on configurations, vulnerabilities and credentials remains confidential. The report is delivered only to the controller; credentials do not appear in the documents.                                                                                                                          |
| Who can stop everything         | A contact named by Voltaria can ask for immediate suspension at any time. Every session begins and ends with a notice to the contact.                                                                                                                                                                     |
| Retention of evidence           | Encrypted copy kept for twelve months, then destroyed with a certificate; test devices securely erased within thirty days of closure (chapter 23.3).                                                                                                                                                      |

NOTE

Any doubt on these points must be cleared before signing, not after. This document is a demonstration: names, dates and references are fictitious, and the text of a real mandate must be drafted and reviewed with a legal professional.