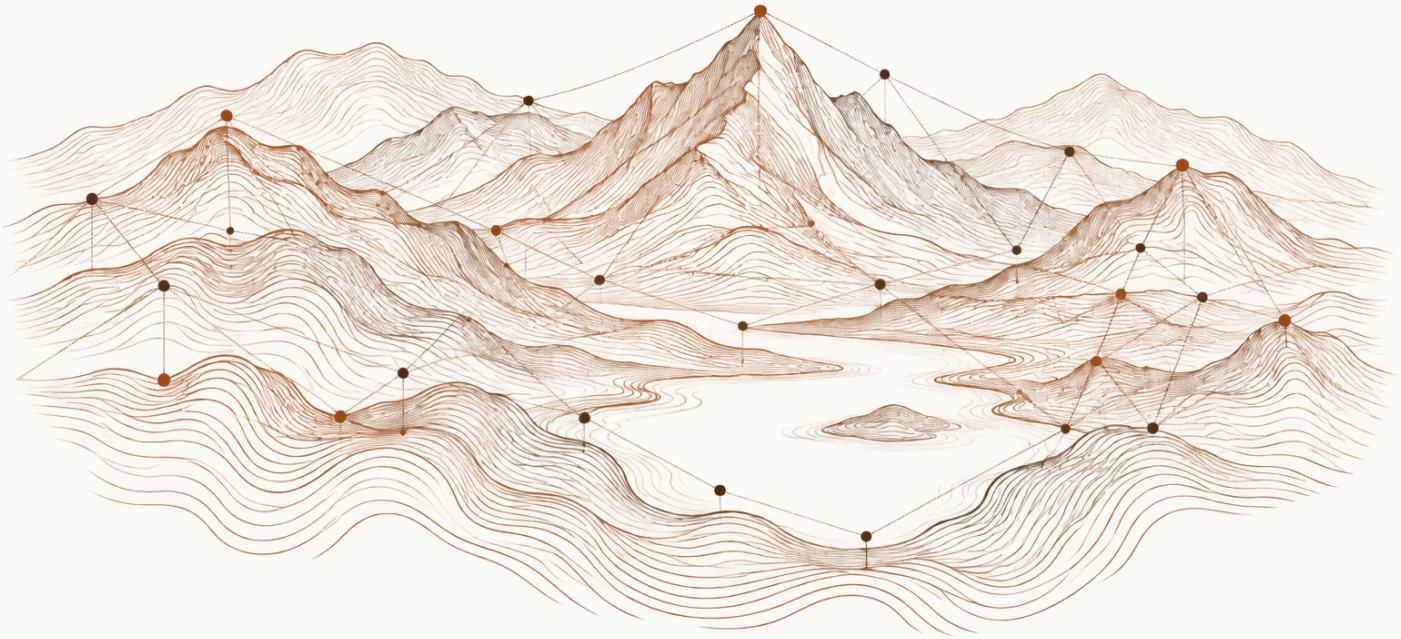
Network Infrastructure Assessment

Valmer Industrie

01 September 2026 - 05 September 2026
Prepared by Vulnotes Security Consulting
Version 1.0.0
CONFIDENTIAL



01 Document control

Version	Issued	Author	Review
1.0.0	2026-09-17	Julien Perrin	Sophie Roux / 16 September 2026

Authorized distribution

Restricted distribution. Intended roles: Marc Lefevre, infrastructure lead; Julien Perrin, assessment author; Sophie Roux, quality reviewer.

This report describes observations within the agreed scope and assessment period. Subsequent changes may affect its conclusions. Distribution is restricted to authorized recipients.

Revision history

Version 1.0.0 issued 2026-09-16. Initial assessment period 1-5 September 2026; editorial review completed 16 September 2026. No remediation retest has yet taken place.

Table of Contents

02 Executive assessment

Assessment opinion

3 findings affect Demonstration office / administration and user zones: 1 High, 2 Medium, 0 Low. The assessment reviewed the agreed configuration and application records against the approved service baseline. Correction priorities reflect the impact, required access and dependencies documented in each finding.

Recommended sequence

Assign F-1 to Marc Lefevre, infrastructure lead for correction by 30 September 2026. Address F-2 and F-3 by 16 October 2026, then perform the documented acceptance checks before closure.

Supporting observations

The network register identifies system owners and distinguishes user, administration and service zones.

Assessment analysis

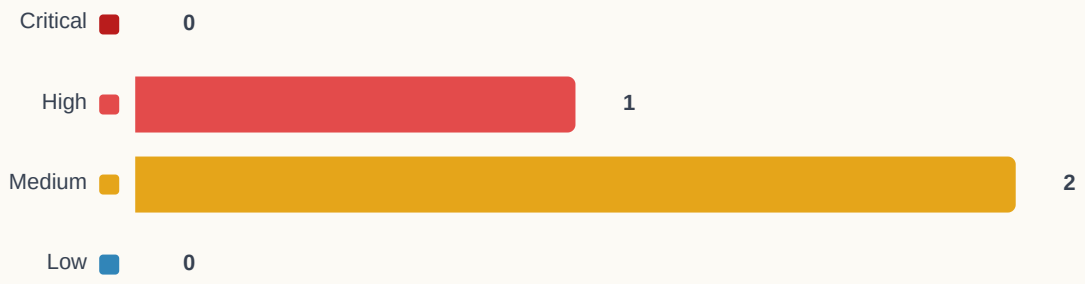
The assessment of Demonstration office / administration and user zones identified 3 findings: 0 Critical, 1 High, 2 Medium, 0 Low. Two documentation-only network ranges, twelve inventory entries and six inter-zone policy rules. Configuration review and reachability records; industrial controllers, wireless access and disruptive validation excluded.

The principal improvement concerns management access policy includes the general user zone. A compromised user workstation could reach management services that should be isolated behind the administration boundary. Correction ownership rests with Marc Lefevre, infrastructure lead. The priority is to reduce this exposure without interrupting the service's required business functions.

The remaining observations concern configuration backups have not been restoration-tested and administrative events are absent from central monitoring. They require separate acceptance criteria because changing one policy does not establish that the other controls operate effectively. Review effective runtime behavior as well as the saved configuration.

The network register identifies system owners and distinguishes user, administration and service zones. These controls provide a basis for remediation, but their presence does not compensate for the documented exceptions. The action plan separates implementation evidence from successful retest results.

Risk distribution



03 Scope and conditions

The following register defines the assessed assets, access conditions and accountable owners.

Zone / asset	Observation point	Expected boundary	System owner
Demonstration office / administration and user zones	192.0.2.0/24 and 198.51.100.0/24 documentation networks	Management access restricted to the administration zone	Marc Lefevre, infrastructure lead

Detailed scope register

Two documentation-only network ranges, twelve inventory entries and six inter-zone policy rules. Configuration review and reachability records; industrial controllers, wireless access and disruptive validation excluded.

Exclusions and restrictions

Only the supplied staging assets and evidence are in scope. Production changes, disruption, social engineering and third-party systems are excluded. Sampling does not establish complete coverage.

04 Assessment coverage

Record the method, reference version, observation date and supporting evidence for each assessed area. A reference mapping does not constitute certification.

Assessment area	Status	Evidence / reference
Asset inventory and ownership	Verified	E-00: twelve owned inventory entries
Service exposure	Gap observed	E-01: management exposure
Expected and observed segmentation	Gap observed	E-01: inter-zone policy
Administrative access	Gap observed	E-01: management sources
Configuration maintenance	Gap observed	E-02: restoration assurance
Monitoring and resilience	Gap observed	E-03: event-source coverage

Allowed statuses: Verified, Gap observed, Not tested, Not applicable. Justify exclusions and not-applicable decisions.

Coverage rationale

Configuration and documentary evidence were reviewed from 1 to 5 September 2026. Each observation is linked to E-01, E-02 or E-03. Areas without evidence remain Not tested; a successful sampled check does not imply coverage of the entire environment.

Reference: engagement baseline DEMO-2026-09, revision 1.0, approved for this engagement.

05 Environment context

Assessed environment

Demonstration office / administration and user zones. 192.0.2.0/24 and 198.51.100.0/24 documentation networks. Service ownership: Marc Lefevre, infrastructure lead. The evidence bundle is frozen at assessment close; later changes are outside this issue.

Evidence requirements

Record source and destination zones, asset identifiers, protocol, observation time and expected policy. Distinguish confirmed reachability from assumed exposure.

Evidence register

E-01: E-01: two redacted policy rules and zone matrix, reviewed 3 September 2026. Production probes were outside scope.

E-02: E-02: backup job inventory and recovery register, 4 September 2026; twelve scheduled jobs, zero recorded restoration exercises.

E-03: E-03: twelve-device inventory compared with nine registered central sources, 5 September 2026.

06 Findings register

Findings use the report order. Keep the same reference in the action plan and retest record.

F-1 Management access policy includes the general user zone

FINDING F-1	High / Not applicable

F-2 Configuration backups have not been restoration-tested

FINDING F-2	Medium / Not applicable

F-3 Administrative events are absent from central monitoring

FINDING F-3	Medium / Not applicable

Management access policy includes the general user zone

FINDING F-1	High / Not applicable

Observation and affected context

Two management-access rules include the general user zone rather than the approved administration zone. The supplied reachability matrix corroborates the broader permitted boundary.

Technical analysis

The policy includes ordinary user endpoints in the permitted source boundary for management services. Effective access depends on rule ordering, expanded address objects and device-local controls, not only a rule label. The supplied zone matrix corroborates the broader boundary without establishing administrative authentication success.

Affected scope and limits

Two rules are in scope. The documentation ranges identify zones and must not be treated as real targets. The assessment does not assert weak management credentials, a remotely exploitable service or successful device administration.

Impact

A compromised user workstation could reach management services that should be isolated behind the administration boundary.

- Trust separation: a user endpoint can reach a service plane that should be reserved for controlled administration.
- Business exposure: workstation incidents and administration-plane incidents are less effectively separated. The High rating reflects the management boundary, while actual administrative action would still depend on additional authorization or a separate weakness.

Correction

Restrict management sources to the approved administration zone, review dependencies and verify required access with the system owners.

1. Resolve source and destination groups and restrict management access to the approved administration path, with named exceptions and accountable owners.
2. Review rule ordering and equivalent device-local access controls. Preserve necessary monitoring and emergency support paths through the approved change process.
3. Log administrative access decisions at useful boundaries and reconcile the network policy with the asset register after deployment.

Accountable owner: Marc Lefevre, infrastructure lead. Preserve release and rollback evidence before requesting closure.

Supporting evidence

F-1 / Management access policy includes the general user zone

evidence record

E-01: two redacted policy rules and zone matrix, reviewed 3 September 2026. Production probes were outside scope.

E-01 / NETWORK INFRASTRUCTURE

Reviewed item	Scope	Recorded state
Policy sample	6 inter-zone rules	2 management rules too broad
Expected boundary	Administration zone	General user zone excluded

Evidence register / Review window: 01-05 September 2026

E-01 - Reviewed record extract, September 2026.

Acceptance criterion

Management services remain available from the administration zone and are denied from the user zone.

Closure evidence to collect

1. Review the corrected effective policy and an owner-approved, non-disruptive zone-access matrix.
2. Confirm required administrative access remains available and ordinary user-zone access is denied.
3. Retain rule identifiers, review timestamps and approval evidence; do not infer full segmentation assurance from these two corrected rules.

Retest status: pending. These are planned validation requirements, not successful test results. Record the corrected version, review date, owner and residual exceptions before closure.

CVSS: not applicable. This is a control-assurance or hardening observation without an independently characterized exploit path. Its contextual risk rating remains applicable.

Management policy target

```
source_zone: administration
destination_group: management
service_group: approved-management
logging: enabled
```

References

Engagement baseline DEMO-2026-09, revision 1.0; evidence E-01.

NIST SP 800-41 Rev. 1 - firewall policy

Configuration backups have not been restoration-tested

FINDING F-2	Medium / Not applicable

Observation and affected context

The twelve sampled devices have backup jobs, but the recovery register contains no completed restoration exercise for the current configuration generation.

Technical analysis

A successful backup job demonstrates collection, not recoverability. A usable recovery chain also depends on configuration compatibility, software versions, key material, licensing and access to recovery documentation. None of these should be assumed solely from a scheduled-job status.

Affected scope and limits

Twelve devices have scheduled backups, but the current configuration generation has no recorded restoration exercise. This is an assurance gap: it does not prove that the backup files are corrupt or that a recovery attempt would fail.

Impact

The organization cannot demonstrate that configuration backups support the expected recovery time.

- Availability: an incident may take longer to resolve if missing dependencies or undocumented steps are discovered only during recovery.
- Integrity and continuity: an incomplete configuration restoration could reintroduce obsolete policy or omit required services. No measured recovery time is claimed because no exercise result was supplied.

Correction

Schedule a controlled restoration exercise in a representative spare environment and record recovery steps, dependencies and timings.

1. Choose representative device families and document required software, dependencies, configuration integrity checks and authorized recovery access.
2. Restore a current backup into an isolated spare or equivalent non-production environment. Prevent accidental reconnection with duplicated production identities or routing.
3. Record functional verification, elapsed recovery time and deviations, then update the runbook and repeat after material platform changes. Protect backup confidentiality and separate backup access from ordinary device administration.

Accountable owner: Marc Lefevre, infrastructure lead. Preserve release and rollback evidence before requesting closure.

Supporting evidence

F-2 / Configuration backups have not been restoration-tested

evidence record

E-02: backup job inventory and recovery register, 4 September 2026; twelve scheduled jobs, zero recorded restoration exercises.

E-02 / NETWORK INFRASTRUCTURE

Reviewed item	Scope	Recorded state
Backup coverage	12 sampled devices	12 scheduled jobs
Recovery evidence	Current configuration generation	0 recorded restoration exercises

Evidence register / Review window: 01-05 September 2026

E-02 - Reviewed record extract, September 2026.

Acceptance criterion

Restore a representative configuration successfully and obtain owner approval of the measured recovery procedure.

Closure evidence to collect

1. Retain the backup version identifier, integrity-check result and target software compatibility record.
2. Validate the restored configuration against approved interfaces, policy and monitoring requirements in the isolated environment.
3. Have the service owner compare measured recovery results with the business objective and approve remaining gaps or corrective actions.

Retest status: pending. These are planned validation requirements, not successful test results. Record the corrected version, review date, owner and residual exceptions before closure.

CVSS: not applicable. This is a control-assurance or hardening observation without an independently characterized exploit path. Its contextual risk rating remains applicable.

References

Engagement baseline DEMO-2026-09, revision 1.0; evidence E-02.

NIST SP 800-34 Rev. 1 - contingency planning

Administrative events are absent from central monitoring

FINDING F-3	Medium / Not applicable

Observation and affected context

Three sampled management devices are not present in the central log-source register. Local event records exist, but no central ingestion evidence was supplied.

Technical analysis

Local administrative events are not evidenced at the central collection boundary for three devices. Source configuration, transport, parsing and indexing form a chain: presence in a source register alone does not establish that usable records reach detection or investigation workflows.

Affected scope and limits

The inventory contains twelve devices and the central register contains nine. This discrepancy supports a monitoring-coverage gap, not proof that local logging is disabled. No historical compromise or deliberately suppressed record is asserted.

Impact

Administrative changes on these devices may not be visible during centralized detection or investigation.

- Detection: administrative changes on the missing sources may not contribute to central alerting and correlation.
- Investigation: local records may be unavailable after device loss, rotation or reconfiguration. Missing timestamps or unstable source identifiers would further weaken correlation even after ingestion is enabled.

Correction

Onboard the missing event sources, define retention and verify ingestion and alert ownership with a benign administrative event.

1. Configure approved forwarding for the three missing sources and use authenticated, protected transport where supported by the platform.
2. Normalize source identity, event category, actor and time zone; verify time synchronization and retain the original event where needed for interpretation.
3. Assign ownership for ingestion health, retention and alerts. Monitor silence and parser failures, not just the existence of a configured collector.

Accountable owner: Marc Lefevre, infrastructure lead. Preserve release and rollback evidence before requesting closure.

Supporting evidence

F-3 / Administrative events are absent from central monitoring

evidence record

E-03: twelve-device inventory compared with nine registered central sources, 5 September 2026.

E-03 / NETWORK INFRASTRUCTURE

Reviewed item	Scope	Recorded state
Inventory	12 management devices	9 registered central sources
Gap	3 devices	Local events; central ingestion not evidenced

Evidence register / Review window: 01-05 September 2026

E-03 - Reviewed record extract, September 2026.

Acceptance criterion

All twelve devices appear in monitoring, and a benign administrative event is searchable with its correct timestamp and source.

Closure evidence to collect

1. Record a benign, approved administrative event on each onboarded source and confirm central searchability.
2. Compare original and indexed timestamps, actor fields and source identifiers; check for truncation or parsing loss.
3. Confirm all twelve sources have a current ingestion status and that monitoring owners receive a controlled health notification.

Retest status: pending. These are planned validation requirements, not successful test results. Record the corrected version, review date, owner and residual exceptions before closure.

CVSS: not applicable. This is a control-assurance or hardening observation without an independently characterized exploit path. Its contextual risk rating remains applicable.

References

Engagement baseline DEMO-2026-09, revision 1.0; evidence E-03.

NIST SP 800-92 - computer security log management

07 Remediation and retest

Finding	Owner / target	Status	Acceptance evidence
F-1 to F-3	Marc Lefevre, infrastructure lead / 30 Sep-16 Oct 2026	Open; retest pending	Finding-specific acceptance checks in the action plan

Action plan

F-1: Marc Lefevre, infrastructure lead. Target 30 September 2026. Management services remain available from the administration zone and are denied from the user zone.

F-2: Marc Lefevre, infrastructure lead. Target 16 October 2026. Restore a representative configuration successfully and obtain owner approval of the measured recovery procedure.

F-3: Marc Lefevre, infrastructure lead. Target 16 October 2026. All twelve devices appear in monitoring, and a benign administrative event is searchable with its correct timestamp and source.

Retest record

Not retested as of 16 September 2026. Proposed retest window: 19-20 October 2026, subject to delivery evidence. All three findings remain Open; no correction or risk acceptance is asserted.

08 Rating and limitations

Rating method

Technical vulnerabilities use CVSS v3.1. Each scored finding includes its vector and prerequisites. Business priority also considers exposure and service dependencies. Control-assurance and governance observations are rated contextually and marked Not applicable for CVSS. CVSS is owned by FIRST and used by permission.

Residual uncertainty

Conclusions apply to the recorded configuration versions and assessment window. Untested areas are listed in the coverage register. Changes after evidence collection require revalidation. All findings remain open until the documented acceptance evidence has been reviewed.

Technical severity and remediation priority may differ. Document the reason when exposure, business context or correction dependencies change the order of work.