VARNYXIS

DEMONSTRATION REPORT

External Security Exposure Assessment

Customer: **NorthSea Transport Solutions — DEMO COMPANY**

Reporting date	2026-11-09
Reference time	2026-11-08 00:00:00 UTC (fixed laboratory reference)
Data	Varnyxis Security Lab v1 — synthetic scenarios
Prepared by	Varnyxis (early-stage project, not yet a commercial service)
Contact	contact@varnyxis.com · varnyxis.com

SYNTHETIC DEMONSTRATION — NO REAL SYSTEMS WERE ASSESSED

NorthSea Transport Solutions is a fictional company. All assets use documentation-only IP addresses (RFC 5737) and reserved .example domains. The findings come from synthetic laboratory scenarios; no scanning, log-in attempt, exploitation or other network activity took place.

Classification: DEMONSTRATION MATERIAL — fictional data, may be shared for evaluation

Version 1.0

EXECUTIVE SUMMARY

What this demonstration shows

A plain-language overview for the business owner. Everything in this report is synthetic: it shows what a Varnyxis Exposure Monitor report could look like, not the state of real systems.

What was simulated

We assembled 8 items from 10 scenarios of the Varnyxis Security Lab, a synthetic laboratory with fictional companies and data, and present them as if they belonged to one fictional customer. In the laboratory, the assets belong to separate fictional organizations.

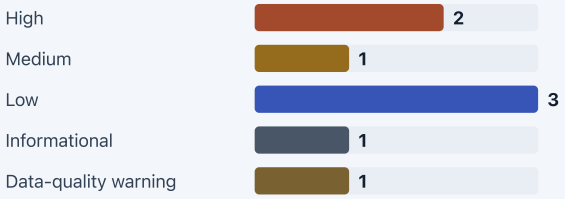
What deserves attention

6 items are worth discussing with the customer: remote desktop reachable from the internet (high), a database service reachable from the internet (high), an expired TLS certificate on the customer portal (medium) first, then lower-priority e-mail and software-version topics.

What is fine

The public website on HTTPS is expected and has no concern. An old record that mentioned remote desktop is *not* reported as current, because newer data supersedes it.

Selected items by priority



Priority is a triage order for follow-up, not a vulnerability severity score.

1 new exposure found between two checks

2 fixes confirmed by a later check (one later came back)

1 issue that came back after being fixed

What cannot be concluded

- No system is shown to be vulnerable, breached or exploited. An open service is an exposure to review, not proof of a weakness.
- The CVE item is an **unverified association** based on a version label; it may not apply.
- Nothing here describes real infrastructure: the data and changes are synthetic dataset snapshots.

Synthetic demonstration — no real systems were assessed. Findings, dates and confidence levels are reproduced from Varnyxis Security Lab v1 without alteration; see the appendix and report-evidence-map.json for traceability.

SCOPE AND METHODOLOGY

How the assessment was produced

Synthetic demonstration — no real systems were assessed. No real network activity took place: no scanning, no log-in attempts, no exploitation, no live vulnerability verification and no penetration testing.

Data sources (all synthetic)

- Synthetic passive internet-scan records (ports, services, versions)
- Synthetic DNS records (SPF, DMARC)
- Synthetic TLS certificate records
- For the appendix examples: synthetic owner package inventory, alert feed and configuration review

Fictional assets in scope

10 assets: documentation-only IP addresses (192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24) and reserved `.example` domains. In the laboratory, each asset is authorized through a trusted inventory; assets outside it are rejected before analysis.

Assessment period

Observations dated 2026-09-01 to 2026-11-05 (one superseded record from 2025). All time-dependent checks use the fixed reference time **2026-11-08 00:00:00 UTC**, never the current clock.

How items are classified

CLASS	MEANING
Observed exposure	A service is reachable from the internet. It shows exposure only, not a weakness.
Potential configuration concern	An exposure that usually should not exist (e.g. remote desktop, databases). A hypothesis for review.
Unverified CVE association	A data source links a reported version to a CVE. Not proof of vulnerability or exploitability.
Configuration defect evidenced by the synthetic record	The record itself shows the defect (e.g. an expired certificate date, a DMARC policy of p=none). Confirmed only within the synthetic ground truth.

Priority and confidence

Priority orders follow-up work (high, medium, low); it is not a CVSS severity. **Confidence** reflects the evidence: the lower of the finding type's maximum and the reliability of its source. A single passive scan record gives medium confidence; a direct DNS or certificate record gives high; a version-based CVE association is always low.

ASSET AND EXPOSURE OVERVIEW

What was observed, where and when

Each row is one Security Lab v1 fixture record (19 records, 10 scenarios), classified from that record alone. All sources are synthetic; addresses are documentation-only and domains are reserved `.example` names. “Check” is the dataset snapshot (S1 earlier, S2/S3 later). “Defect” = configuration defect evidenced by the synthetic record; an exposure shows reachability, not weakness.

ADDRESS / DOMAIN	SERVICE / RECORD	PORT	SOURCE	OBSERVED	CHECK	CLASSIFICATION	LAB
203.0.113.12	RDP	3389	Passive scan	2026-11-02	S1	Exposure — potential concern	LAB-02
198.51.100.13	PostgreSQL 16.4	5432	Passive scan	2026-11-03	S1	Exposure — potential concern	LAB-03
lab06-logistics.example	SPF / DMARC	—	DNS record	2026-11-05	S1	Defect: DMARC p=none	LAB-06
192.0.2.17	TLS certificate	443	TLS certificate	2026-11-01	S1	Defect: certificate expired	LAB-07
192.0.2.17	HTTPS · nginx 1.26.2	443	Passive scan	2026-11-01	S1	Informational (web service)	LAB-07
203.0.113.19	HTTPS · Apache httpd 2.4.49	443	Passive scan	2026-11-04	S1	Informational (web service)	LAB-09
192.0.2.23	RDP	3389	Passive scan	2025-06-01	S1	Superseded (not current)	LAB-13
192.0.2.23	HTTPS · nginx 1.26.2	443	Passive scan	2025-06-01	S1	Superseded (not current)	LAB-13
192.0.2.23	HTTPS · nginx 1.26.2	443	Passive scan	2026-11-03	S1	Informational (web service)	LAB-13
198.51.100.14	HTTPS · nginx 1.26.2	443	Passive scan	2026-11-04	S1	Informational (web service)	LAB-04
198.51.100.14	TLS certificate	443	TLS certificate	2026-11-04	S1	Informational (valid to 2027-03-01)	LAB-04
lab19-freight.example	SPF / DMARC	—	DNS record	2026-09-01	S1	Defect: DMARC p=none	LAB-19
lab19-freight.example	SPF / DMARC	—	DNS record	2026-10-01	S2	No concern (SPF, DMARC p=reject)	LAB-19
lab19-freight.example	SPF / DMARC	—	DNS record	2026-11-05	S3	Defect: DMARC p=none	LAB-19
203.0.113.27	HTTPS · nginx 1.26.2	443	Passive scan	2026-10-01	S1	Informational (web service)	LAB-17
203.0.113.27	HTTPS · nginx 1.26.2	443	Passive scan	2026-11-05	S2	Informational (web service)	LAB-17
203.0.113.27	RDP	3389	Passive scan	2026-11-05	S2	Exposure — potential concern	LAB-17
lab18-logistics.example	SPF / DMARC	—	DNS record	2026-10-01	S1	Defect: no SPF record	LAB-18
lab18-logistics.example	SPF / DMARC	—	DNS record	2026-11-05	S2	No concern (SPF, DMARC p=quarantine)	LAB-18

SECURITY FINDINGS (1/3)

Findings and observations

8 items. Priority orders the follow-up; it is not a severity rating, and no item is a confirmed vulnerability.

F-01 Remote desktop (RDP) reachable from the internet — High

Lab source	LAB-02
Asset	203.0.113.12:3389
Observed	2026-11-02
Classification	Observed exposure — potential configuration concern
Priority	High
Confidence	medium
Status	Open

Evidence. Remote Desktop Protocol (version not reported) reported on TCP/3389 (rdp) at 203.0.113.12. No CVE association, no authentication information. (Synthetic passive internet-scan record)

Possible business impact. Internet-facing remote desktop is a frequently abused entry point. If an account uses a weak or reused password, an attacker could reach internal systems.

Recommended next action. Confirm whether remote desktop must be reachable at all. Close TCP/3389 to the internet and offer access through a VPN or remote-desktop gateway with multi-factor authentication. Review authentication logs.

Verification limitations. Authentication settings (Network Level Authentication, MFA, account lockout) cannot be seen passively. No log-in was attempted. There is no evidence of compromise.

F-02 Database service reachable from the internet — High

Lab source	LAB-03
Asset	198.51.100.13:5432
Observed	2026-11-03
Classification	Observed exposure — potential configuration concern
Priority	High
Confidence	medium
Status	Open

Evidence. PostgreSQL 16.4 reported on TCP/5432 (postgresql) at 198.51.100.13. No CVE association, no authentication information. (Synthetic passive internet-scan record)

Possible business impact. A database that is reachable from the internet is exposed to password guessing and to any weakness in its configuration. Databases normally only need to be reachable from the application.

Recommended next action. Restrict PostgreSQL to the private network or to the application servers only. From the owner side, check pg_hba.conf, listen_addresses, TLS and database roles.

Verification limitations. Whether authentication and TLS are enforced is unknown. No connection to the database was made.

F-03 E-mail domain policy only monitors (DMARC p=none) — Low

Lab source	LAB-06
Asset	lab06-logistics.example
Observed	2026-11-05
Classification	Configuration defect evidenced by the synthetic record
Priority	Low
Confidence	high
Status	Open

Evidence. DNS for lab06-logistics.example: SPF "v=spf1 include:_spf.mailhost.example -all"; DMARC "v=DMARC1; p=none". (Synthetic DNS record)

Possible business impact. Receivers are not asked to reject e-mails that falsely use the company domain, which makes invoice and payment fraud easier. It does not mean the domain has been spoofed.

Recommended next action. Review DMARC aggregate reports, make sure every legitimate sender passes SPF/DKIM, then move to p=quarantine and later p=reject.

Verification limitations. DKIM was not assessed. The record shows the policy only; it does not show whether spoofing has occurred.

SECURITY FINDINGS (2/3)

Findings and observations (continued)

F-04 TLS certificate of the customer portal has expired — Medium

Lab source	LAB-07
Asset	192.0.2.17:443
Observed	2026-11-01
Classification	Configuration defect evidenced by the synthetic record
Priority	Medium
Confidence	high
Status	Open

Evidence. Certificate for portal.lab07-freight.example on 192.0.2.17:443 valid until 2026-10-15; evaluated against the fixed reference date 2026-11-08. Protocols: TLSv1.2, TLSv1.3. (Synthetic TLS certificate record; Synthetic passive internet-scan record)

Possible business impact. Visitors see browser security warnings, which damages trust and teaches users to ignore warnings.

Recommended next action. Renew the certificate now, automate renewal and add an expiry alert at least 30 days in advance.

Verification limitations. The certificate may have been renewed after the observation date. Certificate chain and host-name checks were outside the laboratory scope.

F-05 Web server version associated with a CVE (unverified) — Low

Lab source	LAB-09
Asset	203.0.113.19:443
Observed	2026-11-04
Classification	Unverified CVE association
Priority	Low
Confidence	low
Status	Open

Evidence. Apache httpd 2.4.49 reported on TCP/443 at 203.0.113.19. The data source associates CVE-2099-2001 (fictional identifier). (Synthetic passive internet-scan record)

Possible business impact. If the reported version is accurate and the affected component is enabled, the server may need a patch. The data does not establish this.

Recommended next action. Check the installed package version against the vendor advisory and patch if affected. Document the result either way.

Verification limitations. The association comes from the version shown in the banner only. Banners can be wrong, and vendors often back-port fixes without changing the version (see appendix). Nothing was tested.

F-06 Old remote-desktop record superseded by newer data — Warning

Lab source	LAB-13
Asset	192.0.2.23
Observed	2026-11-03
Classification	Data-quality warning — not a finding
Priority	Warning
Confidence	n/a
Status	Superseded

Evidence. Record of 2025-06-01 showed ports 3389 and 443; newer record of 2026-11-03 shows port 443 only, for 192.0.2.23. (Synthetic passive internet-scan record)

Possible business impact. None for the current state. Reporting the old record as current would be a false alarm.

Recommended next action. No action for remote desktop. Continue monitoring so that a re-opening would be detected.

Verification limitations. The data does not show when the service was closed, only that the newer observation no longer lists it.

SECURITY FINDINGS (3/3)

Findings and observations (continued)

F-07 Public website served over HTTPS

Informational

Lab source	LAB-04
Asset	198.51.100.14:443
Observed	2026-11-04
Classification	Informational observation — no concern
Priority	Informational
Confidence	n/a
Status	No action

Evidence. nginx 1.26.2 on TCP/443 at 198.51.100.14; certificate valid until 2027-03-01; protocols TLSv1.2, TLSv1.3. (Synthetic TLS certificate record; Synthetic passive internet-scan record)

Possible business impact. Expected and acceptable for a company website. Listed so that the report shows what was reviewed, not only what needs work.

Recommended next action. No action needed. Keep the web server updated and certificate renewal automated.

Verification limitations. Only the service and certificate were observed; the website content and application were not assessed.

F-08 E-mail domain policy weakened again after being fixed

Low

Lab source	LAB-19
Asset	lab19-freight.example
Observed	2026-11-05
Classification	Configuration defect evidenced by the synthetic record
Priority	Low
Confidence	high
Status	Reopened

Evidence. DMARC policy of lab19-freight.example over three checks: 2026-09-01 p=none; 2026-10-01 p=reject; 2026-11-05 p=none. (Synthetic DNS record)

Possible business impact. Protection against spoofed e-mails was removed again, which points to a change made without a security check.

Recommended next action. Find out why the policy was changed (often a new mailing service). Configure that sender correctly, restore p=reject and add the DMARC check to the change procedure.

Verification limitations. The data shows the policy at three dates only, not who changed it or why.

CHANGES AND REMEDIATION

What changed between checks

A one-time assessment shows a single moment. Comparing checks over time shows what is new, what was fixed and what came back.

ID	CHANGE	ASSET	BETWEEN CHECKS	TYPE	LAB
C–01	Remote desktop newly reachable	203.0.113.27	2026-10-01 → 2026-11-05	**new** (alert)	LAB–17
C–02	Missing SPF record published	lab18–logistics.example	2026-10-01 → 2026-11-05	**resolved**	LAB–18
C–03	DMARC moved from p=none to p=reject	lab19–freight.example	2026-09-01 → 2026-10-01	**resolved**	LAB–19
C–04	DMARC set back to p=none	lab19–freight.example	2026-10-01 → 2026-11-05	**recurred** (alert)	LAB–19
C–05	Public website unchanged	203.0.113.27	2026-10-01 → 2026-11-05	**unchanged**	LAB–17

Example: a fix that did not last (LAB-19)



The policy was strengthened and later weakened again. Without repeated checks the regression would go unnoticed until the next audit.

How changes are decided

- **New**: absent before, present now, and the earlier check covered that service or record.
- **Resolved**: only when a later check of the *same* record shows it is fine. Missing data is never treated as a fix.
- **Recurred**: present again after having been resolved.
- **Unchanged**: present in both checks.

> These are changes between **synthetic dataset snapshots**, not observed changes to real infrastructure.

RECOMMENDED ACTION PLAN

What to discuss with the customer

A practical list for the IT provider. Varnyxis does not perform remediation; it reports, prioritizes and re-checks.

ID	FINDING	RECOMMENDED ACTION	PRIORITY	RESPONSIBLE PARTY	VERIFICATION REQUIRED	STATUS
C-01	**Remote desktop newly reachable (203.0.113.27)**	Same as F-01: close TCP/3389 to the internet or move behind VPN/gateway with MFA; check which change opened it.	High	IT provider, with customer approval	External re-check; change record reviewed	Open (new)
F-01	**Remote desktop (RDP) reachable from the internet**	Confirm whether remote desktop must be reachable at all. Close TCP/3389 to the internet and offer access through a VPN or remote-desktop gateway with multi-factor authentication. Review authentication logs.	High	IT provider (firewall / remote access), with customer approval	External re-check shows 3389 closed; firewall rule documented	Open
F-02	**Database service reachable from the internet**	Restrict PostgreSQL to the private network or to the application servers only. From the owner side, check pg_hba.conf, listen_addresses, TLS and database roles.	High	IT provider or hosting provider	External re-check shows 5432 closed; access rules reviewed with the owner	Open
F-04	**TLS certificate of the customer portal has expired**	Renew the certificate now, automate renewal and add an expiry alert at least 30 days in advance.	Medium	IT provider or web hosting provider	Certificate valid beyond the next 30 days; automatic renewal confirmed	Open
F-03	**E-mail domain policy only monitors (DMARC p=none)**	Review DMARC aggregate reports, make sure every legitimate sender passes SPF/DKIM, then move to p=quarantine and later p=reject.	Low	IT provider (DNS / e-mail)	DNS shows p=quarantine or p=reject; DMARC reports show legitimate mail passing	Open
F-05	**Web server version associated with a CVE (unverified)**	Check the installed package version against the vendor advisory and patch if affected. Document the result either way.	Low	IT provider (server maintenance)	Installed package version compared with the vendor advisory	Open
F-08	**E-mail domain policy weakened again after being fixed**	Find out why the policy was changed (often a new mailing service). Configure that sender correctly, restore p=reject and add the DMARC check to the change procedure.	Low	IT provider, with the customer's change process	DNS shows p=reject again at the next check	Reopened

Informational items (F-07) and the superseded record (F-06) need no action and are not listed. Responsible parties are suggestions to agree with the customer.

MONTHLY MONITORING VALUE

How a partner IT company could use Varnyxis Exposure Monitor

Proposed service capabilities. Varnyxis Exposure Monitor is a proposed service and does not exist as a production service. The points below describe what a future monitoring service for *authorized* assets could offer; they are not proven production performance.

Detect changes

Repeated checks of authorized domains and IP addresses, flagging newly reachable services such as the remote-desktop example (C-01).

Follow up on observations

Each item keeps its status (open, resolved, reopened) from one report to the next, so nothing silently disappears.

Explain risks clearly

Plain-language summaries with priority and confidence, and explicit statements of what cannot be concluded.

Track remediation

A fix is marked resolved only when a later check of the same record confirms it (C-02), and regressions are flagged (C-04).

Prepare recurring reports

A consistent monthly report the IT provider can review, adjust and present to its own customer.

What already exists

Only the synthetic Security Lab v1 and this demonstration. Live data sources, scheduling, partner branding and Dutch/French reports are planned, not built.

Principles a partner can rely on

- Only assets the customer has authorized and whose control is verified.
- Passive and permitted data sources; no exploitation and no password attempts.
- Human review before anything is sent to a customer.
- No item is presented as a confirmed vulnerability without verification by the asset owner.

About Varnyxis

Varnyxis is an early-stage cybersecurity automation project developing external security monitoring and reporting for IT service providers. It is not yet a commercial service, has no customers and has not yet been incorporated. Contact: **contact@varnyxis.com** · varnyxis.com

TECHNICAL APPENDIX (1/2)

Traceability and evidence

Every item maps to a Varnyxis Security Lab v1 scenario. The machine-readable version, with fixture record references and ground-truth references, is `report-evidence-map.json`.

REPORT ID	LAB SCENARIO	LAB ITEM KEY	CLASSIFICATION IN REPORT
F-01	LAB-02	rdp_exposed@L02-IP1:3389	Observed exposure — potential configuration concern
F-02	LAB-03	database_exposed@L03-IP1:5432	Observed exposure — potential configuration concern
F-03	LAB-06	dmarc_monitoring_only@L06-DOM	Configuration defect evidenced by the synthetic record
F-04	LAB-07	tls_certificate_expired@L07-IP1:443	Configuration defect evidenced by the synthetic record
F-05	LAB-09	unverified_cve_association@L09-IP1:443	Unverified CVE association
F-06	LAB-13	stale_observation_superseded@L13-IP1	Data-quality warning — not a finding
F-07	LAB-04	public_web_service@L04-IP1:443	Informational observation — no concern
F-08	LAB-19	dmarc_monitoring_only@L19-DOM	Configuration defect evidenced by the synthetic record
C-01	LAB-17	rdp_exposed@L17-IP1:3389	new
C-02	LAB-18	spf_missing@L18-DOM	resolved
C-03	LAB-19	dmarc_monitoring_only@L19-DOM	resolved
C-04	LAB-19	dmarc_monitoring_only@L19-DOM	recurred
C-05	LAB-17	public_web_service@L17-IP1:443	unchanged
A-LAB-10	LAB-10	unverified_cve_association@L10-IP1:22	Not reported (downgraded)
A-LAB-16	LAB-16	legacy_tls_protocol@L16-IP1:443	Not reported (downgraded)

What the system deliberately did not report

LAB	INDICATOR	REASON RECORDED BY THE LABORATORY
LAB-10	CVE association not reported	Owner-provided package inventory shows the fix is backported for every reported CVE; the banner version alone is not evidence.
LAB-16	Legacy-TLS alert downgraded	A low-reliability alert is contradicted by newer, higher-reliability evidence showing only modern TLS versions.

Data handling

In LAB-03 a duplicate record contained a field with a sensitive-looking name; the laboratory rejected the whole record and never copied its values. Raw banners are always discarded; this report contains none.

TECHNICAL APPENDIX (2/2)

Definitions, confidence and limitations

Confidence methodology

Confidence = the lower of (a) the maximum for the finding type and (b) the best reliability of its evidence source. Source reliability: passive scan record *medium*; DNS, TLS, owner-provided records *high*; alert feed *low*. Type maximum: exposures and configuration findings *high*; unsupported software *medium*; CVE associations *low*.

Technical limitations

- All data is synthetic; the laboratory rules and scenarios were written by the same team, so laboratory results show internal consistency, not real-world detection accuracy.
- Rules are simplified: DKIM, SPF lookup limits, cipher suites and certificate host-name matching were not assessed.
- Priority is a triage hint, not a CVSS score.
- Passive data cannot show authentication settings, patch levels or compromise.
- The report combines scenarios of different fictional organizations into one fictional customer for illustration.

Glossary

Exposure	A service reachable from the internet.
RDP	Remote Desktop Protocol, remote access to Windows systems.
SPF / DMARC	DNS records that tell receivers which servers may send e-mail for a domain and what to do with e-mails that fail.
TLS certificate	The certificate behind HTTPS (the browser padlock).
CVE	Public identifier of a known vulnerability. CVE IDs in this report use the fictional year 2099.
Back-port	A security fix applied without changing the version number.
Superseded record	Old data replaced by newer evidence.
Reference time	The fixed date used for all time checks, so results are reproducible.

Synthetic demonstration — no real systems were assessed. NorthSea Transport Solutions is fictional. Documentation-only IP addresses and .example domains only. Produced from Varnyxis Security Lab v1 (20 synthetic scenarios); no independent third-party testing has taken place.