External Attack Surface Report

Sample (demo) deliverable for clients — Excel + PDF package

Client	ACME S.L. (sample)
Scope	empresa.com (and discovered subdomains)
Report date	2026-01-14
Prepared by	Proactive Defender — Intelligence & Exposure Team

Executive summary

This report summarizes externally exposed assets and high-priority security findings identified through passive discovery, service fingerprinting (banners/TLS/headers) and vulnerability intelligence correlation. The intent is to provide an actionable remediation plan, prioritizing items with the highest expected impact.

Assets	Open services	High	Medium	Low
12	**27**	**4**	**6**	**9**

Top prioritized findings

Priority	Asset	Evidence	Risk drivers	Recommended action
HIGH	admin.empresa.com:3000	Grafana login exposed	Public admin panel exposure	Restrict by VPN / IP allowlist. Enforce SSO + MFA.
HIGH	staging.empresa.com:8080	Swagger / OpenAPI accessible	API surface leakage	Disable public docs in production. Require auth + rate-limit.
HIGH	203.0.113.10:22	OpenSSH fingerprint detected	Remote admin exposed	Keys-only auth. Restrict source IPs. Disable passwords.
HIGH	mail.empresa.com:25	SMTP banner reveals product/version	Targeted exploitation	Patch MTA. Disable weak ciphers. Add monitoring.

Scope and methodology

Scope: Primary domain empresa.com. Discovered subdomains were included where they resolved to public IPs. Scanning was limited to lightweight fingerprinting (banners/TLS/headers) and did not include intrusive exploitation.

Method: (1) Asset discovery, (2) Service identification, (3) Fingerprinting, (4) Vulnerability intelligence correlation (CVE/KEV/EPSS), (5) Risk scoring and prioritization.

Asset inventory (sample)

Asset	IP	Open ports	Notes
api.empresa.com	203.0.113.10	443, 22	Public API endpoint
app.empresa.com	203.0.113.11	443, 80	Web application
admin.empresa.com	203.0.113.12	3000, 443	Admin panel exposure
staging.empresa.com	203.0.113.13	8080, 443	Non-production reachable from Internet
mail.empresa.com	203.0.113.14	25, 587, 993	Mail services

Risk scoring model (summary)

Risk score is a normalized value (0.0–1.0) computed from: CVSS base severity, evidence confidence, exposure (public reachability), and exploitation likelihood signals (CISA KEV and EPSS where available).

Vulnerability details (sample)

The following entries illustrate how findings appear in the PDF. The full technical list is also delivered in the Excel file with sortable columns (asset, service, CVE, CVSS, KEV, EPSS, evidence, recommendation).

CVE	Asset / service	CVSS	KEV	EPSS	Risk	Recommendation
CVE-2024-XXXX	admin.empresa.com:3000 (Grafana)	9.8	Yes	0.42		Patch to fixed version. Restrict public access.
CVE-2025-YYYY	api.empresa.com:443 (nginx)	7.5	No	0.08	0.61	Update nginx. Add WAF rule and monitoring.
CVE-2023-ZZZZ	mail.empresa.com:25 (MTA)	8.1	No	0.17	0.68	Patch MTA. Disable weak TLS ciphers.
CVE-2022-WWWW	203.0.113.10:22 (OpenSSH)	6.8	No	0.05	0.52	Harden SSH config. Restrict by IP and disable passwords.

Remediation plan (30-60-90 days)

Timeline	Focus	Actions
0-30 days	Reduce immediate exposure	Close/limit admin panels. Remove public staging. Enforce strong auth on remote access.
30-60 days	Patch and harden	Patch high-risk CVEs. Standardize TLS configs. Add monitoring and alerting for changes.
60-90 days	Operationalize	Automate periodic scanning. Integrate findings into ticketing. Establish SLA for remediation.

Appendix

Data fields included in the Excel deliverable

The Excel report contains structured tables with the following columns (varies by sheet): asset, ip, port, protocol, banner evidence, TLS metadata, detected product/version, matched CVE, CVSS, KEV flag, EPSS score, confidence, risk_score, and recommended action.

Limitations

This is a sample report. In production, results depend on the agreed scope and the currently observable exposure. Fingerprint-based correlation can produce false positives/negatives; confidence scores are provided to help triage. If you require intrusive verification, it must be explicitly authorized.