Managed Vulnerability Scanning
By CyPro

ANNOTATED SAMPLE

Sample Vulnerability Scan Report

A worked example of the monthly report our clients receive, with margin notes explaining why each part reads the way it does. Every organisation, host, address and finding in this document is fictitious.

How to read this sample: the structure below is the report a real client receives each cycle. The data is invented for a fictional company, Harborview Interiors Ltd, so nothing here describes any real system. Notes marked "Why it reads this way" are annotations for you, the evaluator; they do not appear in a live report.

CLIENT	Harborview Interiors Ltd (fictitious)
SCAN CYCLE	Monthly, external. Cycle 7 of the engagement
ESTATE IN SCOPE	14 external IP addresses, 22 resolvable hostnames
RAW SCANNER RESULTS	187 reported items
AFTER CONSULTANT TRIAGE	8 findings worth your attention: 1 critical, 2 high, 3 medium, 2 low
MOVEMENT SINCE LAST CYCLE	5 fixed, 1 outstanding, 2 new

Why it reads this way: the gap between 187 raw items and 8 findings is the service. Duplicates, informational noise and false positives are removed by a consultant before the report is written, and the ranking that follows reflects real exploitability, not just the scanner's severity label.

The ranked fix list

#	FINDING	AFFECTED ASSET	PRIORITY	STATUS
1	VPN appliance running firmware with a publicly exploited vulnerability	vpn.harborview.example (203.0.113.10)	Critical, fix first	New this cycle
2	Administration interface for the CMS reachable from the internet	www.harborview.example (203.0.113.12)	High	New this cycle
3	Mail gateway accepts a deprecated TLS version	mail.harborview.example (203.0.113.14)	High	Outstanding, cycle 2
4	Expired certificate on a legacy subdomain still serving content	old.harborview.example (198.51.100.8)	Medium	New last cycle
5	Web server version disclosure in response headers	www.harborview.example	Medium	Accepted risk candidate
6	Directory listing enabled on a marketing microsite	promo.harborview.example (198.51.100.9)	Medium	New this cycle
7	Missing security headers on two public sites	www, promo	Low	Tracked
8	DNS record pointing at a decommissioned service	files.harborview.example	Low	Tracked

Why it reads this way: priority is not a copy of the scanner's severity. Finding 1 outranks everything because the weakness is being exploited in the wild on an asset that faces the internet and gates the whole network. Finding 5 carries a scanner severity of medium, but with no practical attack path it is flagged as a candidate for formally accepting the risk rather than spending patch effort. That judgement, made by a person who can defend it, is what the ranking is for.

Finding write-ups, as your IT team receives them

1 VPN appliance running exploited firmware

What we found: the remote-access VPN at vpn.harborview.example reports a firmware build affected by a vulnerability with public exploit code in active use (reference redacted in this sample). **Why it ranks first:** internet-facing, exploited in the wild, and a successful attack lands inside the corporate network. **Fix:** apply the vendor's patched firmware, then rotate any credentials used on the appliance since the affected build was installed. **Retest:** we rescan on request the moment the patch is applied rather than waiting for the next cycle.

2 CMS administration interface exposed

What we found: the content management login for the main website answers to the whole internet, protected only by a password form. **Why it ranks here:** exposed admin interfaces are a standing target for credential stuffing; one reused password ends in a defaced or hijacked site. **Fix:** restrict the path to your office and remote-work addresses at the web server or move it behind the VPN; enable multi-factor authentication on all CMS accounts either way. **Retest:** confirmed closed when the path stops answering externally.

Why it reads this way: each write-up gives the person doing the work everything they need in four sentences: what, why it matters, the fix, and how closure is proven. Longer technical appendices exist for teams that want them, but the fix list never depends on reading one.

The trend, cycle on cycle

CYCLE	OPEN FINDINGS	FIXED	NEW	OLDEST OPEN FINDING
Cycle 5	14	3	4	62 days
Cycle 6	11	6	3	48 days
Cycle 7 (this report)	8	5	2	34 days

Why it reads this way: this table is what an auditor, an insurer or a board member actually wants: proof that exposure is measured, managed and falling. For ISO 27001 control A.8.8, Cyber Essentials Plus readiness and PCI DSS evidence, the dated cycle-on-cycle trail does the work that a one-off report cannot.

Removed before you saw them

This cycle the consultant discarded 179 raw items: 112 informational entries, 41 duplicates across hostnames sharing one server, 19 findings on services already decommissioned, and 7 false positives verified by hand against the affected hosts. A live report lists these totals so the work is visible; nobody's time is spent reading them.

About this sample

Harborview Interiors Ltd does not exist; addresses use documentation ranges and hostnames use reserved example domains. A live report is produced for your estate every cycle on the band you choose, at the prices published at managedvulnerabilityscanning.co.uk/pricing/. Questions about anything in this sample: hello@cypro.co.uk.