

cyberwhy

SERVICE GUIDE

Vulnerability Assessment

A practical guide to finding known weaknesses, ranking them sensibly and fixing the right things first.

01 · OVERVIEW

Why it matters

A vulnerability assessment is a systematic search for known weaknesses: outdated software, missing patches, insecure settings and exposed services. It gives you a map of where you are exposed, across many systems at once.

Its strength is breadth and repeatability. Its real value is not the list itself, but the ranking: which few findings deserve work this week, and which can wait.

Typical triggers

- You have no current overview of what is exposed
- The patching backlog keeps growing and priorities are unclear
- An audit, customer questionnaire or tender asks for regular assessments
- A new environment, cloud migration or acquisition adds systems
- You run AI workloads, containers or new model-serving infrastructure
- You want a regular security health check

Who benefits

IT manager
A prioritized to-do list instead of a flood of alerts.

Security lead
A baseline and a trend over time.

Operations
Clear instructions on what to patch or reconfigure.

Compliance lead
Documented, repeatable assessments.

In this guide

01 Overview 2
02 What it is, and what it is not 3
03 How it works, step by step 4
04 What you receive 5
05 In practice 6
06 How to prepare 7
07 Questions, references and terms 8
08 How the services fit together 9

02 · SCOPE

What it is, and what it is not

What it is

- + A broad, largely automated search for known weaknesses
- + Reviewed by specialists, so false alarms are removed
- + Repeatable, so progress can be measured
- + Focused on what to fix first, not on the longest list

What it is not

- – Not a penetration test: it does not prove what an attacker can actually exploit
- – Not a one-off cure: new weaknesses are published continuously
- – Not a list to fix all at once
- – Not a certification

What can be assessed

Networks

Which hosts and services are reachable, which versions run, and which known weaknesses they carry. Internal and external views.

Applications

Web applications and their components, checked for common weaknesses and vulnerable libraries.

Systems and configuration

Operating systems, servers and devices, checked for missing patches, weak settings and unnecessary services.

Modern environments

Where in scope: cloud services, containers and the infrastructure that serves AI workloads.

Ways to scan

Unauthenticated

Scanning from the outside, as an attacker sees it. Fewer findings, closer to real exposure.

Authenticated

Scanning with an account. Finds missing patches and settings that are invisible from outside.

Recurring

The same scope scanned regularly, so changes and progress become visible.

03 · PROCESS

How it works, step by step

A typical engagement, from the first conversation to clear next steps. Exact steps and timing are agreed with you when the work is scoped.

01 Discuss

Understand the environment and the reasons behind the assessment.

- Clarify the goal: baseline, audit, change or concern
- Get an overview of networks, applications and systems
- Learn which systems are business critical

YOU PROVIDE
The environment and your reasons
A technical contact

YOU GET
A clear brief

02 Scope

Agree what is covered, and nothing else.

- List networks, applications and systems in scope
- Decide on authenticated or unauthenticated scanning
- Agree time windows so scans do not disturb operations
- Agree how results are shared and stored

YOU PROVIDE
What is in scope
Accounts for authenticated scans, if agreed

YOU GET
An agreed scope

03 Scan

Find known weaknesses systematically.

- Discover the assets in scope
- Scan for known vulnerabilities, outdated software and misconfigurations
- Run in the agreed time windows with controlled load

YOU PROVIDE
Access to the agreed scope

YOU GET
Raw findings

04 Analyze

Separate what matters from noise.

- Check each finding and remove false positives
- Put findings in context: exposure, exploitability and importance of the system
- Rank by priority, so the most critical risks come first

YOU PROVIDE
Answers about which systems matter most

YOU GET
Prioritized findings

05 Report

Make the results usable for the people who fix them.

- Write a detailed analysis of what was found
- Give recommendations per finding and per group of findings
- Order the work by priority

YOU PROVIDE
Nothing further

YOU GET
A detailed analysis and prioritized recommendations

04 · DELIVERABLES

What you receive

The analysis is built for action: it groups findings by cause, so one patch or one setting closes many entries at once, and it orders the work by priority.

01
Overview
Scope, method and the overall picture in plain language.

02
Asset view
Which systems were found and where the findings concentrate.

03
Detailed findings
What is wrong, where, and why it matters.

04
Priority ranking
The order in which to work, with reasoning.

05
Recommendations
Concrete steps: patch, reconfigure, remove or replace.

06
Support for standards
Material that supports work toward GDPR, ISO 27001 and NIST requirements.

How priority is decided

Severity	**How bad**	The technical severity of the weakness, commonly scored with CVSS.
Exposure	**How reachable**	Is the system reachable from the internet, or only from deep inside?
Exploitation	**How likely**	Is the weakness already used by attackers, or is exploit code public?
Importance	**How valuable**	What does the system do, and what data does it hold?

A severity score is only a starting point. Priority combines four questions, so the list reflects your situation rather than a generic scale.

05 · IN PRACTICE

Seeing it at work

From findings to fixed, as a routine

1 Group
Combine findings by cause: one update or one setting often clears dozens of entries.

2 Schedule
Patch in planned windows, critical systems first, and note exceptions with a reason.

3 Verify
Scan again to confirm the weakness is gone and nothing new appeared.

4 Repeat
Run the same scope on a regular cycle, and compare results to see progress.

EXAMPLE OF A FINDING (FORMAT ONLY)

Outdated web server version on a public host

High

AFFECTED	Public web server, version several releases behind
DESCRIPTION	The installed version has known weaknesses fixed in later releases.
PRIORITY REASONING	Reachable from the internet, a public exploit exists, the system hosts a customer-facing service.
FIX	Update to a supported version, then confirm with a repeat scan.

FOR AI PROJECTS

Assessing projects that use AI

AI projects bring new infrastructure: model servers, vector databases, notebooks, pipelines and many open source components. They often start as experiments and stay exposed. An assessment makes them visible and checks for outdated components, open ports and default settings.

06 · PREPARATION

How to prepare

A little preparation makes the work faster, safer and more useful. Here is what helps most.

Before we start

- Collect a list of networks, domains and systems
- Name the systems that are most important to the business
- Decide on time windows for scanning
- Prepare accounts if authenticated scans are wanted
- Tell your hosting provider, if required
- Decide who will receive and fix the findings

Typical ground rules

- + Only the agreed scope is scanned
- + Scans run in the agreed time windows
- + Results are confidential and shared only with named people
- + Scan accounts have the minimum rights needed

Common misconceptions

~~We patch automatically, so we are fine.~~	**In practice:** Automatic patching misses unmanaged systems, third-party software and insecure settings.
~~One assessment a year is enough.~~	**In practice:** New weaknesses are published continuously, and systems change. Regular assessments show the trend.
~~Everything critical must be fixed today.~~	**In practice:** Ranking exists so that limited time goes to the few things that carry the most risk.

07 · REFERENCE

Questions, references and terms

Frequently asked questions

How is this different from a penetration test?
An assessment finds known weaknesses broadly. A penetration test shows what can actually be exploited. They complement each other.

Will scanning disturb our systems?
Scans are run in agreed time windows and with controlled load. Sensitive systems can be handled separately.

How often should we assess?
Regularly, and after major changes. The cycle depends on how fast your environment changes.

What are false positives?
Findings that look like weaknesses but are not. Specialists check findings so you do not spend time on them.

Do we need to give you accounts?
Only if you want authenticated scans, which find more. Accounts get the minimum rights needed.

Can this support an audit?
The analysis supports work toward standards such as ISO 27001, GDPR and NIST. It is evidence of a process, not a certification.

Reference frameworks and sources

CVE and NVD	The public catalogs of known vulnerabilities and their details.
CVSS (FIRST)	The common scale for scoring severity.
CISA Known Exploited Vulnerabilities	A list of weaknesses known to be used in attacks, useful for priority.
CIS Benchmarks	Hardening guidance for operating systems and software.
NIST SP 800-40	Guidance on planning enterprise patch management.

Terms in plain language

Vulnerability. A weakness that could be used to harm a system.

CVE. A public identifier for a known vulnerability.

False positive. A finding that turns out not to be a real weakness.

Patch. A software update that fixes a weakness.

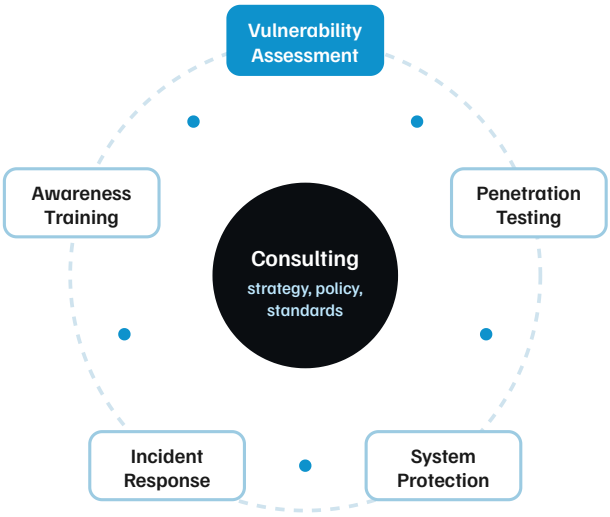
Misconfiguration. A setting that leaves a system less secure than intended.

Baseline. The starting picture that later assessments are compared with.

08 · NEXT STEPS

How the services fit together

Security works best as a cycle: find weaknesses, test them, protect, prepare to respond and keep people alert, all guided by a strategy. You can start with any one of them.



Vulnerability Assessment (this guide)
Finds known weaknesses across your systems and ranks them.

Penetration Testing
Shows what an attacker can actually exploit.

System Protection
Closes gaps with layered, maintained defenses.

Incident Response and Forensics
Acts when something gets through, and learns from it.

Security Awareness Training
Prepares the people who meet threats first.

Cyber Security Consulting
Sets strategy, policy and standards that tie it together.

Talk to a specialist about vulnerability assessment.

Tell us what you are working on and what you need to protect.

EMAIL
info@cyberwhy.com

WEB
cyberwhy.com/services/vulnerability-assessment/

This guide describes how work of this kind typically runs. Scope, methods, timing and deliverables are agreed with you for your situation, and nothing in it is a guarantee. References to standards and frameworks are for orientation and do not mean certification. © CyberWhy. All rights reserved.