

■ AUDIT

Finding It Before Someone Else Does: What an Audit Reviews

Many security reports read like a list of fears. Dozens of findings, all in red, none with context. They are good for justifying a purchase, not for deciding where to start on a Monday.

A review worth having answers three questions in plain language: what could happen, how likely it is in your case, and what it costs to close.

Where We Start

- What is exposed to the internet that nobody remembers publishing.
- Access still held by people who no longer work with you, and keys shared between several.
- Pending updates on what holds the business up, not on the entire inventory.
- Backups: whether they exist, whether they restore, and when that was last tested.

Pentesting Is Not the Same as an Audit

An audit looks at configuration and agreements. A pentest tries, with written scope and permission, to use what it finds to show how far someone could get. The second makes sense once the first is in order. Otherwise you are paying to confirm the obvious.

What You Get

A short, prioritised report: what we found, what makes it possible, and what we recommend doing first. Plus a conversation to go through it, because the hardest part of any report is understanding what it means for your operation.

We work with written scope and authorisation, on systems the client owns. There are no guaranteed findings: there is an honest account of what turned up within that scope.