The Best Security Architects Know How Systems Break

By: Jaiz Anuar

21 July 2026 · Cybersecurity · Security Architecture · 7 min read

Great security architects understand how attackers think, so they can design systems that remain resilient when trust fails.

When people think about cybersecurity architecture, they often imagine secure networks, security controls and solution diagrams. All are important. But great security architects also understand how systems break.

Not because they want to break them, but because they understand how attackers think.

Every Attack Reveals An Architecture Decision

Attackers rarely create new weaknesses. More often, they discover weaknesses that already exist: overly trusted service accounts, exposed management interfaces, forgotten APIs, excessive permissions, flat networks and missing trust boundaries.

These are architecture decisions. Every successful attack tells a story about a design assumption that turned out to be wrong. The best security architects learn from those stories before they become incidents.

Thinking Like An Attacker Improves Design

A Red Team does not simply ask whether a server is secure. It asks: if I compromise this server, where can I go next?

This shifts the focus from protecting individual systems to protecting trust relationships between systems. Good architecture is not about making every component impossible to compromise. It is about ensuring that when one component fails, the entire environment does not fail with it.

Secure By Design Starts Before Deployment

Many organisations rely on testing near the end of a project, when findings lead to controls that fix symptoms rather than underlying design. Secure by Design begins during architecture, design discussions and threat modelling, before the first line of code is written.

Changing a diagram is always easier than changing a production system.

Security Architecture Is More Than Technology

Understanding how systems break is only part of the equation. A security architect must also understand business objectives, operational constraints and governance requirements.

The goal is not to design the most secure environment imaginable. It is to design an environment that remains secure while enabling the business to operate effectively.

Final Thoughts

Not every Red Team member will become a security architect, and not every architect needs years of offensive experience. But every security architect should develop an attacker's perspective.

Every attack path reveals a design decision. Every exploited vulnerability exposes an assumption. Every incident offers an opportunity to build stronger architecture.

The best security architects are recognised because they understand how trust can be broken—and how to design systems that remain resilient when it is. That is where Secure by Design truly begins.

Question assumptions. Share knowledge. Build trust.