Security Think Tank: Walk before you run

How can organisations combine software-defined networking, containerisation and encryption to prevent rogue code from running freely across a corporate network?

We have all tested this postulate: "One needs to first walk before running." This applies in life as well as in cyber security. I have seen many companies buying shiny and blinking boxes without first addressing fundamental controls, and then failing to receive the promised value from these investments.

Having said that, the paradigm of zero-trust networks, software-defined datacentres and containerisation delivers an exceptional level of security through automation, asset management, self-healing policies and application partitioning.

However, as with anything in IT and cyber security, an exceptional technology operated by untrained and undisciplined people following not-so-well thought through and documented processes is bound to fail. Even worse, a false sense of security could mean higher likelihood of successful attacks.

For companies to benefit from these advanced technology patterns, they need to rethink their processes, eliminating the human element as much as possible, rethink security policies by moving more to industry standards rather than bespoke and, most importantly, train people to use, manage and monitor new technologies.

The key controls should still be implemented even when having these advanced technologies:

- An accurate and detailed CMDB [configuration management database] structured from business processes down to infrastructure.
- A real-time vulnerability and threat management programme.
- Secure baseline builds and automated reporting/remediation of compliance failures.
- Well-designed identity and access control – ideally expressed as a code and linked into a single source of truth of identities, roles and organisational structure.
- Monitoring of events for unusual, out-of-norm events with a follow-up process.

There is more, but these present an absolute minimum to be able to reach the level of benefit promised in your business case for investment into zero-trust networks, software-defined datacentres and containerisation.

Think of this when sitting on a supplier's call showcasing the magic of their technology. There are no shortcuts in life, cyber security included.