

[Five things I learned at InfoSec](#)

Breadcrumb

1. [Home](#) /
2. [Print](#) /
3. [Pdf](#) /
4. [Node](#) /
5. [Entity Print](#)

Insight navigation

- [Latest insights](#)
- [Latest news](#)
- [Articles](#)
- [Case studies](#)

[Download PDF](#)

Jul 2023

Five things I learned at InfoSec

Last month, [Infosecurity Europe](#) came to ExCeL London for three days of knowledge sharing, connecting and rethinking around the power of information security.

Categories Technology Consulting, Cyber Security Strategy, Security Solutions, Security Manager as a Service, Managed Security

Jul 2023

-
-
-
-



[Dan Morrison](#)

Lead Solutions Architect: Security

Email

dan.morrison@waterstons.com

Dan Morrison, one of our [solutions architects](#), once again went along to learn more about upcoming trends, the latest technology, and what other organisations have been up to, as well as catch up with peers and vendors from throughout the industry.

Here are the top five things he learned (or re-learned) while he was there...

1. Zero Trust is becoming more tangible

It's a common buzzword in the security space, but every company – even individual – has their own interpretation of how to achieve it. Honestly, InfoSec taught me that there isn't an exact science; there isn't one way to do it, BUT it is moving away from being simply a concept/mindset with more vendors than ever aligning to create solutions that deliver tangible results.

This hopefully means that while many are striving for the same goal with different approaches – which is totally fine, after all a company must do what is right for them – there is becoming more consistency and clarity around what Zero Trust actually looks like for future adopters.

2. Say it with me: Security from the start!

When it comes to application and software security, this needs embedding from the start. To me, this is obvious, but it seems to be commonly missed during development.

There's been a shift in market focus, or at least more options provided, in the realm of software development security; making sure code is secured while it's being written, making sure you're only using secure open-source code (or being notified when a flaw is identified), and making sure your whole software development lifecycle/pipeline maintains secure throughout meaning the end result is ready for launch!

3. Together Everyone Achieves More

Just like raising a baby, security takes a village. From cyber to software, technicians to team leads, every area must be involved to ensure that not only is security embedded from the start (as above), but consistently monitored, tested and updated as a product or service develops. Without this holistic approach, vulnerabilities and weaknesses could grow – or go unnoticed for too long - leading to costly upgrades, patching or even breaches.

4. It's good to talk

It's not often you get the world's leading security experts and providers in one place, so when they are it can lead to some excellent conversations and meetings.

I was fortunate to catch up with the team at AlienVault at their partner appreciation event, and I really enjoyed chatting to them about the latest activities and how we can better serve our clients, gain feedback on our partnership, and collaborate with others to ultimately build a bigger, better understanding around the part they play in information security.

What was incredible to hear was how well our MSSP offering is performing, meaning we're keeping more and more business, even more safe than ever.

5. Footwear and fitness count

Imagine running from gate 1 to 49 at an airport. Through crowds, groups chatting, people trying to get your attention or entice you with goodies. That's what getting from one seminar to another is like.

ExCeL is HUGE. Wear trainers, train in preparation. It's the only way.

To find out more about our technology solutions team and how they can support your business [visit the page here](https://waterstones.com/print/pdf/node/8590).

<https://waterstones.com/print/pdf/node/8590>