Teach them to fish

Cybercrime is on-going, but many breaches could be prevented according to Niroshan Rajadurai. **Bethan Grylls** finds out why business know-how is the key

Last year was dubbed the "worst ever" by the Online Trust Alliance for data breaches and cyber incidents around the world. Interestingly, it revealed that 93% of the breaches recorded in 2017 could have been prevented. And with cybercrime continuing to make the headlines, this year hasn't seen much improvement. Niroshan Rajadurai, director of sales and field engineering EMEA at Semmle, software specialists, believes that industry is going wrong and failing to address the problems of cybercrime correctly.

"Software is 'eating' the world" Rajadurai explains. "Right now, we're in the Software Age. Digitalisation is being embraced by more businesses all the time; companies are taking traditional processes and integrating Internet of Things (IoT) capabilities into them."

Although software proliferation is opening up a range of possibilities for businesses and customers, Rajadurai suggests that it is also one of the biggest challenges for software developers, because it's opening doors for hackers too.

"If you go to your friend's house, you can leave your mobile on the table and know if you came back in a few hours, it should still be there," Rajadurai says. "If you did the same at a shopping centre, there's no guarantee your mobile will still be there when you returned.

"It's the same concept," he suggests, "a company has written a piece of software with the expectation it will be in a self-contained, safe environment. For businesses to keep up with the velocity of digitisation we're seeing today, they're using the same software but it's entering a non-self-contained area."

He continues, "The issue is that these older processes weren't designed to be connected and as such, are vulnerable to attacks. Just one weak link in a system can expose you to cybercriminals."

So why not simply discard the old technology if it isn't up to par?

"To simply throw away technology is a non-starter, for one thing that would be extremely expensive," Rajadurai explains. "Companies are left with no choice but to keep the technology they have and find a quick way to scale it to better address the changing requirements of their markets."

Rajadurai believes the explosion of software has been, in part, driven by online retailers like Amazon.

"Businesses are having to "transition", moving from a manual process, where it oversees applications and web servers, to an automated method of service," he says. "This is pushing the need for software which is required to deliver this automation." The concern, however, is that this demand is pressurising companies to deliver automated services too quickly and, as a result, security is not being properly addressed.

The skills gap isn't helping the problem either, stresses Rajadurai. "The number of software engineers isn't growing at the same pace as the volume of software, and this poses a big challenge with regards to building software efficiently and reliability".

In an effort to strengthen business cybersecurity, Semmle offers businesses consultancy services which aim to help them reduce the time, effort and cost of verifying and validating systems.

"Traditionally, businesses have had to rely on vendors to provide updates – that is 'bug fixes' - with no control over when this would be delivered. I strongly believe in giving people the power to control their own destiny.

"Our approach is to put 'helpful' technology in front of these companies and teach them the skills they need in order to deploy and manage their systems securely. This means they can protect themselves without relying on specific individuals or a third party for support."

Variant attacks

One particular issue Rajadurai highlights is 'variant attacks' – a tactic where hackers use public bug updates as a means to finding vulnerabilities in other areas of a company's technology.

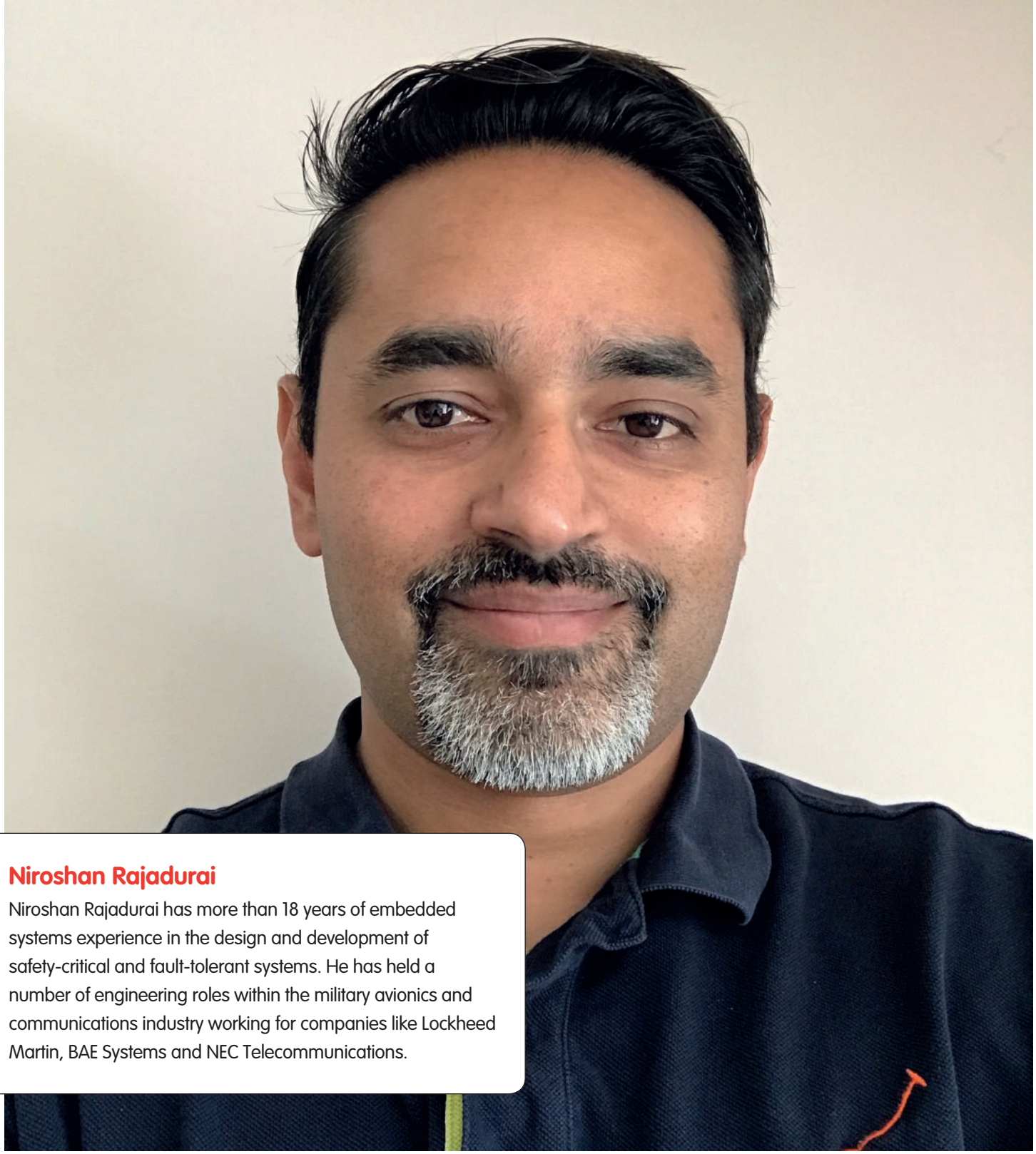
"If a company makes a fix and pushes it out there, they've immediately told the world 'we've got an issue'," Rajadurai explains.

To avoid such attacks, some businesses have started to go through what Rajadurai calls a 'diagnosis fix cycle'. This involves carrying out an analysis on the architecture to see if the same problem is occurring elsewhere, talking to developers, and doing a manual code review. "This approach is, however, very time-consuming", he notes, and it's a problem with a double-edge sword.

"Fix the one identified problem quickly and tell hackers there may be a way to get into the system," Rajadurai says. "Don't fix the problem and the process goes from taking a day to weeks or even months."

Rajadurai thinks Semmle's 'variant analysis' could hold the key. "We automate the process," he says. "We take a company's source code and convert it into a database where questions can be asked.

"Once a vulnerability is discovered in your source code, either reported by externals (bug bounty), through internal review or through root cause analysis after an incident or breach, it's essential to detect and eliminate all semantically similar - but often syntactically very different - vulnerabilities that exist across the application portfolio. Failure to do so exposes the organisation to additional risk from malicious attackers.



Niroshan Rajadurai

Niroshan Rajadurai has more than 18 years of embedded systems experience in the design and development of safety-critical and fault-tolerant systems. He has held a number of engineering roles within the military avionics and communications industry working for companies like Lockheed Martin, BAE Systems and NEC Telecommunications.

After the vulnerability is identified, a 'query' can be constructed. QL, a type of declarative, object-oriented query language, ships with extensive libraries and abstraction features that enable you to write advanced queries without having to worry about low-level language concepts and compiler specifics. "Instead," Rajadurai says, "you can focus on investigating and interrogating your own codebases."

The QL finds logical variants of the same error elsewhere in the code. The code is then 'captured' before it gets merged, preventing similar vulnerabilities from being introduced in future and "giving businesses results in days rather than weeks or months".

He continues, "Software isn't going to slow down. We need to keep developing tools and keep up with the speed in which it's is being built.

"Cybersecurity has given a new meaning to quality. It doesn't just affect the brand now, but it opens doors to more serious issues.

"Quality deficiencies have become a way of attacking businesses and stealing and exploiting data. It is no longer simply about whether a device or service can deliver its solution to a high standard, but also whether it can deliver it without opening itself or its customer to additional risks.

"These companies know they have a problem," he clarifies, "but they don't know how to manage that problem. The answer is teaching them the best way to address it."