

The cybersecurity resource problem

Four ways to get proactive

Talented cybersecurity resources have always been difficult to find, expensive to procure, and hard to retain. COVID-19 has exacerbated the cybersecurity skills shortage, and proactive security has been put on the back burner for many companies, exposing gaps in their cybersecurity resources

Here are four ways to strengthen your cybersecurity position:

01 Establish internal security training and certification programmes

True cybersecurity requires a cultural shift. Every employee should take part in security education and certification programmes. Develop meaningful and relevant programmes that engage employees and help them understand cybersecurity threats and their roles in mitigating them. 'Lunch and learns', mock breaches, and escape rooms are all great ideas

02 Promote security cross-pollination

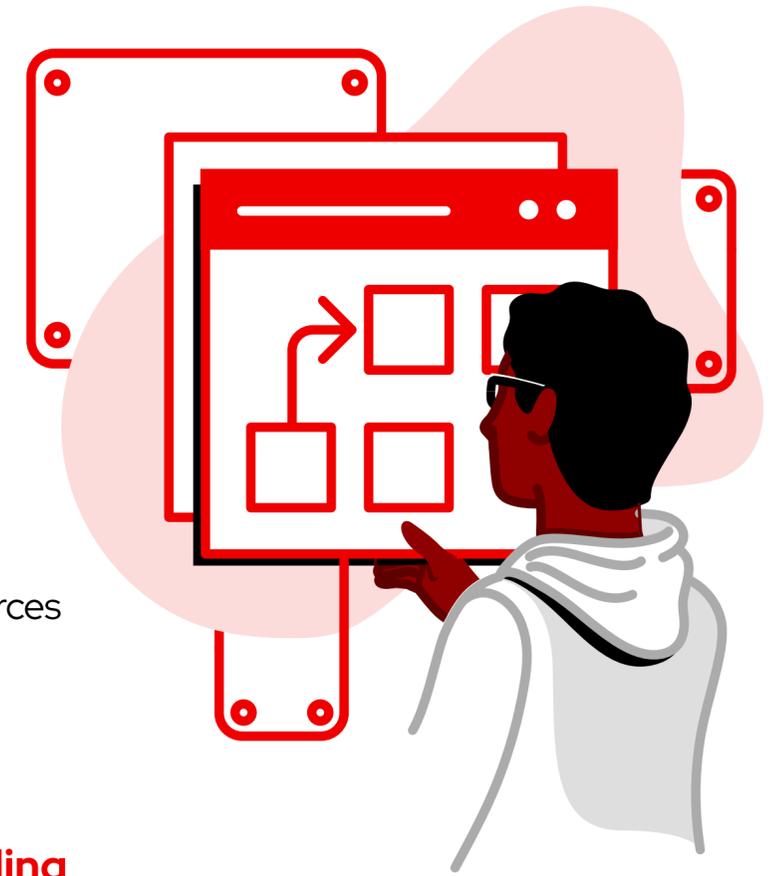
If security is everyone's job, then security resources should not be limited to the IT department. Think about ways security can cross-pollinate within the business. This develops a company-wide understanding of security issues and encourages collaboration and the opportunity to build security into processes, products, and services from the ground up

03 Take a hard look at security tooling

A thorough inventory of existing security tooling will reveal what's needed (and not needed) to address current security concerns. Many organisations have security tools they don't need or that are out of date and can't support new technologies, such as cloud, containers, or Kubernetes. This wastes time and money

04 Put a consistent automation strategy in place

As IT environments and the world become more complex, so do the security events facing IT teams; no human or group of humans could ever address every security threat. A consistent automation strategy can help organisations more effectively mitigate risks by reducing human errors, remediating issues, responding quickly to security alerts, and developing repeatable security and compliance workflows. Look for an approach that overlays a consistent automation strategy across app dev, infrastructure, and security operations



The tools for success



Proactive planning, strategic technology implementation, and widespread, ongoing, and engaging security awareness training and collaboration will go a long way in addressing and managing the cybersecurity resource problem

