

VIEWPOINT

The Value Of Evaluation

In a world where all information security companies are claiming ‘the most secure’, ‘the most professional’, and ‘the most knowledgeable’, Kevin Sheldrake looks into the benefits of trustworthy third-party evaluations

Everyone wants the best. When they can't afford the best, everyone wants value for money. But to compare ‘value’ for ‘money’, we must be able to rate ‘value’ in terms of ‘money’, i.e. pounds. This leads to a problem in the information security market as we don't tend to have that many benchmarks, and the ones we have seem to be ignored or misunderstood by the vast majority of companies. So how do we compare and achieve ‘value for money’? It's all in seeking third party evaluation and certification and, luckily, the Government has set the standard.

In Cheltenham, within the walls of the infamous GCHQ, lives an organisation known as the Computer-Electronics Security Group, or CESG for short. They are recognised by the Government as the National Technical Authority for all things cryptographic and electronic security, including IT and information security. They advise Government, Defence, and Industry on threats and countermeasures and are, quite simply, the best in the country, if not the world. In order to provide their advice and endorsements as wide as possible they operate a number of evaluation and certification schemes that range from products and systems through to consultants and penetration testers:

(1) Use of Certified products: CESG act as the Certification Body for UK product evaluations under ITSEC and as the UK arm of Common Criteria. Products that have been evaluated and certified are identified as providing a certain level of assurance in the functionality that was tested. ITSEC uses E-numbers (from 1 to 6) and CC uses EAL-numbers (from 1 to 7). CC numbers are generally one higher than ITSEC numbers and the benchmark evaluation for trusted barriers is generally accepted to be ITSEC E3 or CC EAL4. The golden rule is to check what was evaluated, however, as most product evaluations leave out bits of functionality. The detail is in the Target Of Evaluation, which can usually be found on the ITSEC part of the CESG web site, www.cesg.gov.uk. For example, if you were to buy an evaluated proxy firewall to protect your internet connection, you would expect the proxies to be

part of the evaluation but in many cases they are not. I generally urge all firewall buyers to stick to evaluated proxy firewalls and ignore all firewalls that have not had their stateful inspection *and* proxy functionality evaluated. Otherwise you are trusting software that has not been through any third-party check.

(2) System Evaluation by a CESG Licensed Evaluation Facility. A CLEF may be used to provide proof that a system or product has been well designed and implemented, including code reviews and configuration management analysis. They are the only officially trusted third-party systems and product evaluators.

(3) IT Security Health Check by a CESG approved penetration tester. CESG runs the CHECK scheme to provide assurance that a penetration tester will correctly test your system to a prescribed standard. There are a number of CHECK approved companies listed on the CESG web site and I would not recommend using any penetration tester that has not passed the CHECK scheme. There is no other approved scheme for penetration testers so look for that little CHECK badge in their literature.

So what does evaluation buy you? Firstly, there is the confidence that the products or services are as described, an important factor in the security market where anyone can set up as a software developer, consultant, or penetration tester. Secondly, it tends to separate the wheat from the chaff as all self-respecting security companies should seek to gain endorsements for their products and services, and those without endorsements should be eyed with suspicion. Thirdly, it simplifies the security market to the much smaller range of trusted products and services, which can lead to better decisions based on valued judgements instead of the traditional comparison of marketing blurb.

If you are serious about information security you cannot afford to ignore the difference an Evaluated product or service will provide over a rash of unsubstantiated claims. Evaluated assurance levels provide a benchmark that may be used for comparison; all then that is left to argue over is the price.