Corsec

Security Certifications:
Your Human Capital Investment

When considering a product security certification effort, companies are faced with the engineering dilemma, “Should I build it, or should I buy it?”. It is tempting to take the onus of the certification effort on internally as opposed to leveraging a partner; the assumption being that it is the more cost-effective option. This is not always the case; Corsec’s 20-year experience in this area across 400 plus companies globally, has uncovered the human capital investment to be 3 times more expensive when doing this internally versus outsourcing.

Human capital aside, the rigor and stringent timeline of a certification effort often results in internal resources strain, pushback on product release cycles, and delays in go-to-market. With employee disengagement and burn-out rampant across engineering organizations, can companies truly take on the another “distraction” internally?

If you are considering bringing your next certification in-house, take time to evaluate your current resources as you evaluate the additional workload. Even the fully staffed engineering organizations need to plan for the following:

Product Security Hardening

Product Security and QA:

Perhaps the most overlooked, and yet the most important aspect of any security certification effort is ensuring the product complies with the standard and can go through certification successfully. Designing with security inside, defined and documented processes, secure delivery, etc. are all areas which impact the certification effort. Companies need teams of experts skilled in hardware, software, and firmware design, as well as Common Criteria, FIPS 140-2, and DoD APL requirements, as part of their certification team. These experts must analyze the product against current requirements, identifying design gaps that can interfere with the certification process early on in the process, and work with the engineering teams on the plan of record to ensure those gaps are addressed prior to GA of the product.

Development and Vulnerability Testing:

Testing represents another significant portion of the certification effort. Engineers that compose your testing teams are required to conduct a multitude of tests to demonstrate functionality, information assurance, and interoperability of your product. Additionally, they must develop and execute testing against Beta and GA product versions to ensure there is coverage for all security requirements. Prior to testing, members of this team are charged with setting up the product and configurations for evaluations.

Testing varies based on the desired certification, testing teams must operate in specialty groups to address the complex requirements associated with each effort, including, CAVP Algorithm Testing, SHIM Development, Entropy Design, and STIG Testing.

Technical Writing and Engineering Review:

Technical documentation authors need to be highly trained on engineering and cryptographic requirements. They are responsible for evaluating the product and authoring the multiple technical documents required for certification. Documentation is an enormous piece of the certification process, and since labs are responsible for reviewing and approving many of these documents, your efforts must be nothing short of precise, as poorly crafted documents will cause major delays.

Each document must be thoroughly reviewed by people steeped in product security consulting. This panel determines if a document is ready for lab review. The technical review team expedites the certification process, prevents unnecessary delays due to poorly written documents, and mitigates errors which could increase costs associated with lab review.

Product Planning

Industry and Standards Expertise:

FIPS 140-2, Common Criteria and the DoD's APL are not static standards. Each year the governing organizations update these standards many times to reflect changing vulnerabilities, new government guidance, and an ever-evolving landscape. Having internal capabilities with team members who work with governing agencies like NIST, allows you to be on the forefront of standard development processes.

Commercial and Government Go-To-Market:

Certification ROI and business impact are typically measured in financial, brand, and reputation terms. Central to achieving the highest ROI for any certification effort, are market planning, certification and product timing, and leveraging certifications to create a competitive advantage.

Your team needs experience within your relevant industries (government, healthcare, infrastructure, Internet of Things, etc.) to advise you on how to develop and implement go-to-market strategies that work. Your team must be well versed in certifications, timelines, and requirements to ensure successful certification marketing.

Program Management:

The sheer amount of information and resources associated with certification efforts can be overwhelming. The timely nature of these efforts requires every part of the process stays on track. A certification effort often involves product management, product engineering, product security architect, project management, sales, external lab testing, and government interaction; activities which may require the coordinated effort of a senior level program management or team of program managers. Deadlines could slip, communications could be disjointed, and a lack of accountability could permeate organizations that do not have centralized control and ownership of a certification effort.

For more information visit www.corsec.com