Achieve Cyber Security with the Help of Common Criteria Certification

Today's industry and government organizations are highlighting cyber security and information assurance as one of their top IT priorities. Cyber threats are presented by both individuals and nation-sponsored groups with intentions spanning the theft of trade secrets, "hacktivism" (the invasion or disruption of systems for activist purposes) and espionage. Similarly, new problems are rising around supply chain integrity, with tampering and counterfeit incidents degrading user confidence. Organizations suffering from such attacks are susceptible to losing control of confidential information and facing millions of dollars in fines or business losses.

The process of achieving a secured infrastructure has become increasingly complicated as a result of today's innovations in cloud services, mobility and collaboration. These new capabilities offer many operational efficiencies and reductions in cost, but they also create additional risks to the network.

As a result, nations are collaborating to evolve a global standard aimed at providing assurance of a basic level of security for networking equipment. Common Criteria, as its known, is the international program that is crucial to ensuring that the equipment purchased by organizations perform and secure at the level of performance advertised. Acclaimed benefits of this unified system of global IT security standards include:

- Improve availability of assessed, security-enhanced IT products
- Improve citizen confidence in network security
- Enhance the cost-effectiveness and efficiency of the evaluation and certification process
- Allow vendors to focus resources on standard requirements for the improvement of security in products
- Increase scale of certified products and technologies available to IT professionals

With distinct benefit gains, organizations should ask themselves: With a wide selection of products, why wouldn't you buy certified?

The Common Criteria Standard

The Common Criteria for Information Technology Security Evaluation is an international standard (ISO/IEC 15408), providing an infrastructure within which participating organizations can specify functional and assurance requirements, vendors can develop and claim specific product qualities and testing facilities can examine products to determine whether they meet those claims. Common Criteria guarantees that the process of specification, execution and assessment of a product has been conducted in a stringent and standardized manner.

Under the program, classified products are tested against the security requirements of Protection Profiles (PPs). All test labs must be in compliance with ISO 17025, the standard used to evaluate the qualification of testing and calibration laboratories. This process provides organizations with reassured confidence in the protection of critical information, and allows for risk reduction within the network without increases in cost.

There are currently 26 nations participating in the Common Criteria program. Evaluation and testing is performed by independent third-party facilities, with certificates of compliance issued by 15 certificate-issuing nations. Over 2,000 certifications have already been issued for IT products.

Through the certification program, participants gain access to a global community of technical experts, who together identify and address threats, as opposed to each nation attempting to deal with each problem on its own. Threat vector solutions become scalable and repeatable, simultaneously reducing the overall cost and risk. Some nations are still pursuing custom security standards, but this sets limits to the amount of available technology while weakening the quality of goods. Given both vendors and consumers must adhere to finite resources, it is practical to use a universal standards-based approach when verifying security features.

Some governments are still in the process of learning to better manage the adoption process in order to maintain low costs and implement timelines to meet the rapid adaptations of cyber attacks. National agencies are also naturally cautious of sharing too much information with otherwise trusted business and technology partners. However, the overriding need to continue to push the Common Criteria program forward is leading to talks on how to improve its efficacy. By creating a more effective, more efficient and more duplicable evaluation process, new broader sets of evaluated products can be created to address evolving threats.

Common Criteria Beyond the Public Sector

The benefits of Common Criteria do not stop at the government level. The certification brings a certain level of quality assurance for enterprise IT buyers, giving those professionals a dependable, stringent and independently verified set of evaluation requirements for their IT investment. Although Common Criteria certification does not guarantee that products are completely free of security weaknesses, it does provide a higher level of objective assurance that the product executes tasks as documented, and that the vendor will back the product to correct flaws if and when they are found.

The certification program offers purchasing organizations an abundance of information that helps to support higher security in their deployment of evaluated products:

- Consumers are able to compare their needs beside the Common Criteria's consistent standards to decide on the level of security required.
- Buyers can be more definitive when determining if particular products meet their specific requirements.
- They can utilize reports about evaluated security features when judging the relative security of competing IT products.

This has resulted in an increased use of Common Criteria evaluations as a purchasing benchmark, providing guidelines for common sets of requirements that can be used to evaluate products that meet both global and local security needs. Vendors can define their products in terms of which evaluations their products have passed. Similarly, consumers can distinguish and communicate their security needs to vendors.

For example, networking industry leader Cisco is discovering that individual customers may not explicitly mandate Common Criteria in their products, but do require demonstrated secure development practices, with requests for audits, showcases and reports. Cisco, which manages the industry's most rigorous compliance program, already meets a number of government product certification requirements, offering a fully compliant, end-to-end network architecture. Subsequently, certifications such as Common Criteria offer a mutual framework within which network administrators can recognize the security capabilities necessary to meet their needs.

Next Steps for Common Criteria

Common Criteria was previously oriented around the assessment of security products, with comprehensive network security remaining a shortfall for many organizations. Major advancements have been made over the last 12-18 months to magnify evaluation criteria to include product security across a broader set of network components. Additionally, Common Criteria has the potential to encompass supply chain security and management procedures.

Evidently, product security must continue to grow to support new technologies such as cloud, mobility, video conferencing and unified communications. Each of these new technologies carries their own implications. No single nation can effectively pinpoint the direction of the next security requirement – risks can change from nominal to critical in days or even hours. By relying on the broader public/private technical communities, however, security requirements can be quickly developed and deployed, meeting the evolving need to respond to challenges as they occur.

The other important area of evolution for Common Criteria is in the supply chain. Global supply chains have become susceptible to attacks at every stage, including fulfilment, circulation, sustainment and removal. According to the US Department of Commerce (2010), 39 percent of agencies and companies faced counterfeit electronics from 2005 to 2008, with the number of encounters increasing each year. The problem is reoccurring: For example, a US Department of Defense investigation in 2011 showed that no less than 93 separate suppliers to the DoD had provided suspicious parts on at least one occasion, and some more than 10 times.

Vendors need to ensure the integrity of the supply chain by merging traditional management practices with auditable, certifiable system security requirements. By joining basic best practices into a definitive approach, participating nations would be able to leverage steady security parameters to greatly reduce the risks associated with the supply chain. This is not a new idea: the Smart Card community is already implementing Common Criteria, where it is being used as the foundation to assure consistent development and manufacturing processes.

Why Not Purchase Certified Products?

Common Criteria is increasingly renowned for its application to every aspect of the network, especially in environments that can be acknowledged as critical infrastructure, in which governments levy strict regulatory requirements to mitigate risk and assure security:

- Financial transaction systems, to meet standards for protecting banking information
- Healthcare, to help meet the HIPAA regulations for information security of medical information
- Electric utilities, which must comply with standards such as NERC CIP in the US
- Service providers, which have found that Common Criteria compliance allows them to reduce risk without increasing costs
- Transportation, for air traffic control and metro systems

The Common Criteria delivers a foundation that immensely improves overall security of the network without customers incurring additional costs. Vendors are leveraging this standard across their portfolios of products, acknowledging that many customers currently depend on this established security framework. With many choices for available network security products, there does not seem to be any reason as to why any business, organization, or government agency should not purchase products that are Common Criteria certified.

For more information on Common Criteria, visit Cisco Government Certifications.