GSMA™

GSMA Services Showcase Live #5

Building Resilience into Network Equipment Security

Wednesday 7 September 2022

Questions	Answers
How are vendor processes assessment and network product evaluation linked?	The auditor assesses the vendor's product development and lifecycle processes. A security test laboratory evaluates the vendor's network product. For each of these activities, a different set of security requirements exist. GSMA NESAS is designed for equipment vendors to have their internal processes assessed for those products they submit to test laboratories for evaluation. The test laboratory will not only run security tests on the equipment. The laboratory will also examine evidence, delivered by the equipment vendor, that demonstrates the vendor followed their own assessed processes to develop the product under evaluation. The evaluation report that is produced by the test laboratory, consists of both test results and evidence evaluation results.
What can we expect to see in NESAS 3.0?	The most significant upcoming change to NESAS will be the addition of a certification component that will result in the security certification of product development and lifecycle management processes and network products. Additional changes will see the introduction of guidelines for the development and adoption of security assurance specifications by organisations other than 3GPP to facilitate the expansion of NESAS to cover network functions not defined by 3GPP. The NESAS Group will also consider aspects such as record retention, peer review of audits and evaluations and the impact of security breaches on audited processes and evaluated products.
Who or what event triggers a network product evaluation?	Each product evaluation is performed against a specific product version/release. The evaluation remains valid for the lifetime of that product version/release. When the vendor issues a new version/release of the product a fresh evaluation of the new version/release is required.
How do you know that vendors will cooperate with the security processes in advance?	NESAS consists of two components: (1) assessment of vendor development & lifecycle processes, and (2) evaluation of network equipment. For an operator, it is key to ask vendors

	to do both: (1) to undergo the assessment, and (2) to evaluate their products. Both these activities result in reports: (1) auditors write an audit report, which demonstrates whether the vendor meets all the requirements for processes. (2) Test labs produce an evaluation report which lists the test results for all tests. The reports will give operators the necessary insights. Operators should require from their vendors during tender processes to adhere to NESAS. Once you as an operator have access to the reports from the NESA web site, you can determine on your own, if the vendor meets your security expectations. If you have this information available for vendor selection, you can make an informed decision. It will be the auditor who needs to be convinced by the vendor, that the vendor has appropriate security processes and that it adheres to them.