Datasheet

Public Cloud Security Audit

viettel security

Neccessity of Public Cloud Security Audit

In recent years, Cloud Computing Services have become quite familiar and are widely applied in many developing countries around the world, with the aim to focus on managing information infrastructure, thus quickly deploying work, reducing costs and increasing scalability security, etc.

Along with the convenience in accessibility and deployment (Availability) are risks related to security and data integrity issues (Confidentiality, Integrity).

Understanding the urgency of information security issues for systems deployed in the cloud, Viettel Cyber Security has researched, supplemented and applied security standards for these systems. They are built on the basis of standards published by organizations around the world, incorporating our experience in the field of cyber security over the past decade. With a team of experienced experts, we will provide customers with the best services, significantly improving the quality of system information security to meet international standards.

Public Cloud Security Audit of VCS

Public Cloud Security Audit Service of Viettel Cyber Security is a service conducted by experienced network security experts, using advanced tools. Our service offers the following benefits:

- Evaluate and advise on architectural information security issues for systems deployed on popular Public Cloud infrastructure (Amazon Web Service, Google Cloud, Microsoft Azure).
- Review & evaluate problems in setting up decentralization & grouping.
- Review & evaluate misconfiguration issues in the used services.
- Review source code used in the service's scenarios (AWS Lambda, Google Cloud Functions, Azure Functions)
- Consult solutions, ways to overcome each detected problem.

Highlights

STANDARDIZED KNOWLEDGEBASE

The foundation of our service is based on the knowledge of experienced experts. The assessment process complies with the internationally standard checklist from the company's documents and especially the CIS Foundations Benchmark, including basically the following 3 standards:

- CIS Amazon Web Services Foundations Benchmark
- CIS Google Cloud Platform Foundation Benchmark
- IS Microsoft Azure Foundations Benchmark

REAL RISK-BASED RESULTS

Assessment results are not only based on checklists, but also are actually evaluated with specific risk information and evidence. The evaluation contents focus on 4 groups:

- Deployment architecture.
- Problems in setting up decentralization and grouping.
- Misconfiguration issues in user services.
- Review source code used in scripting services.

CONSULTATION & DEPARTMENT SOLUTION

Evaluation results not only point out problems, but also provide remedial recommendations, in-depth advice on headerning methods and sustainable deployment architecture. Moreover, for systems that have integrated CICD, there will be additional advice on DevSecOps deployment.

HIGH QUALITY HUMAN RESOURCES

Our experts who deploy Public Cloud Security Audit Service have many years of experience in the field of cyber security. Especially, Viettel Cyber Security with the motto of taking human resources as the root, currently has high-quality in-depth research personnel with lots of international awards such as: Pwn2Own, Microsoft's MVP, Bugcrowd, HackerOne. Deployment personnel meet many international certifications such as CEH, OSCP, AWS Certification, etc.

Public Cloud Security Audit

viettel security

Implementation process

Public Cloud Security Audit of Viettel Cyber Security (VCS) is carried out through these following steps:

STEP	DESCRIPTION	SLA
Step 1	• VCS researched the preliminary survey of the system and agreed on the implementation plan. The input for the effort estimate includes the number of services and the number of instances per service.	• Up to 5 days from receipt of the request for performance
Step 2	• VCS proposes a service implementation plan, the customer approves the plan, the contents include but are not limited to: ◦ Scope of service ◦ How to perform ◦ Implementation personnel ◦ Implementation method: On-site/Remote ◦ Execution time	• Up to 5 days from receipt of the request for performance
Step3	• The customer prepares all assurance conditions including: a detailed list of scope, connection, account and environment to ensure the evaluation process.	• According to the plan
Step 4	• According to the plan, VCS will evaluate the objects within the scope.	• According to the plan
Step 5	• After the assessment, VCS sends the evaluation results and instructions to overcome the indicated weaknesses.	• According to the plan
Step 6	• If the assessment results contain vulnerabilities or weaknesses, the customer will take corrective action according to the instructions. Once the remediation is completed, the customer submits a request for reevaluation of the remediation, following the same steps required for an initial review. The process ends in the following cases: ◦ The results of evaluation and remedial assessment are no longer error-free. ◦ After 2 weeks, customers do not ask to evaluate the corrected errors. ◦ After 2 times of evaluating the repair errors, the customer still has not completed the fix.	• Up to 1 week from receipt of reevaluation request.