Datasheet

クラウドシステムの安全情報を評価するサービス

(Public Cloud Security Audit)

viettel security

クラウドシステムの安全情報を評価するサービスの必要性

最近、クラウド サービス (クラウド コンピューティング サービス (Cloud Computing Services)はおなじみになって、世界でたくさんの発展途上国に広く使用されています。スケーラビリティ　セキュリティ、コストの削減、作業の迅速な展開、情報インフラストラクチャの管理などに集中するためです。

展開とアクセス能力中の便利　(Availability)とももに、セキュリティとデータ完全性 (Confidentiality, Integrity)という問題についての危険です。

ベトテル・サイバーセキュリティ・カンパニー(Viettel　Cyber Security)はクラウドで展開されているシステムの安全情報を確保する事という問題で必要性を理解し、このシステムのグループに対して安全基準についての研究、補欠、適用を実行しています。世界中の組織によって発行された規格と過去 10 年間の情報セキュリティ分野での経験に基づく、基準が設定されています。経験豊富な専門家のチームにより、顧客に最高のサービス品質を提供し、システム情報セキュリティの品質を大幅に向上させて国際基準を満たすようにします。

クラウドシステムの安全情報を評価するサービス

ベトテル・サイバーセキュリティ・カンパニー(Viettel　Cyber Security)でのクラウドのクラウドシステムの安全情報を評価するサービス(Public Cloud Security Audit)は経験豊富なセキュリティ専門家によって実行されているサービスで、高度なツールが使用されているものです。このサービスには、次のメリットがあります。

- 一般的なパブリック クラウド インフラストラクチャに展開されたシステムに対して建築についての安全情報問題を諮問して、評価します。(アマゾン　ウェブ　サービス- Amazon Web Service, グーグルクラウド - Google Cloud, マイクロソフト アズール - Microsoft Azure)
- サブグループ、分限の設定についての問題を評価し、確認します。
- ユーザー　サービスの構成ミスについての問題を評価し、確認します。
- サービスのサービススクリプトが使用されるソース　コードを確認します。（AWS ラムダ - AWS Lambda, グーグル クラウド ファンクション - Google Cloud Function, アズールファンクション - Azure Functions）
- 検出された各問題に対して克服方法と解答を諮問します。

サービスの主な点

知識の標準化

サービスの基礎は経験豊富な専門家の知識を総括する事に基づいています。評価プロセスが会社の材料、特に CIS Foundations Benchmarkから国際標準化チェックリストに遵守します。基本的に次の３つの規格を含みます。

- CIS アマゾン ウェブ サービス基盤ベンチマーク (CIS Amazon Web Services Foundations Benchmark)
- CIS グーグル クラウド プラットフォーム基盤のベンチマーク (CIS Google Cloud Platform Foundation Benchmark)
- ISマイクロソフト アズール基盤のベンチマーク (IS Microsoft Azure Foundations Benchmark)

実際のリスクに基づく結果

評価結果は、チェックリストに完全に基づいているだけでなく、具体的なリスクの証と情報を使用して実際に評価されます。評価内容が次の４つのグループに中心します。

- 開発アーキテクチャ
- サブグループ、分限の設定について問題
- ユーザー サービスの構成ミスについての問題
- サービススクリプトが使用されるソース コードを確認する事

インテンシブな解答、諮問

評価結果は、問題点を指摘するだけではなく、最終成果物がハードニング方法と持続可能な展開アーキテクチャについてのインテンシブな諮問、克服アドバイスを与えます。また、CI/CD統合システムに対してDevSecOps　の実装に関する諮問があります。

高品質の人材

サービス開発人材は安全情報の分野で長年の経験を持っています。特に、ベトテル・サイバーセキュリティ・カンパニーは人材を根幹に据える方針とともに、Pwn2Own、Microsoft の MVP、Bugcrowd、HackerOneなどの多くの国際的な賞を持っている高品質でインテンシブで研究している人材がいます。

クラウドシステムの安全情報を評価するサービス
(Public Cloud Security Audit)

viettel security

サービス開発プロセス

ベトテル・サイバーセキュリティ・カンパニー((Viettel Cyber Security)のクラウドシステムの安全情報を評価するサービス(Public Cloud Security Audit)は次のプロセスに従って実行されます。

ステップ	業務の内容	サービス水準合意
ステップ1	• ベトテルがシステムの予備調査を研究して、開発計画に統一します。工数見積もりの入力には、サービスの数とサービスごとのインスタンスの数が含まれます。	• 実施請求受領後5日以内
ステップ2	• ベトテル(Viettel)がサービス開発計画を提案し、顧客がその計画を承認します。内容は次の事を含みますが、限られないものとします。 - 実施範囲 - 実施方式 - 実施人材 - 実施方法 - 実施期間	• 実施請求受領後5日以内
ステップ3	• 評価プロセスを確実にするために、顧客は環境、アカウント、接続、スコープの詳細リスト、を含む全ての条件を準備します。	
ステップ4	• 計画によって、ベトテルが範囲で対象を評価します。	• 計画により
ステップ5	• 評価の後、ベトテルが指摘された弱点を克服するためのガイドと評価結果を送信します。	• 計画により
ステップ6	• 評価結果が脆弱性と弱点がある場合には、顧客はガイドに従って克服を行います。克服の後、顧客が　最初の評価と同じ手順で克服を再評価請求を送信します。 次の場合にはプロセスが終わりになります: - 評価結果と修正評価は不具合がありません。 - 2 週間後、克服された不具合を再評価請求を送信しません。 - 克服された不具合を二回評価した後、顧客はまだ克服を完了しません。	• 再評価請求受領後1週以内